Faculteit Rechtsgeleerdheid
Universiteit Gent

Academiejaar 2011-2012

OPSPORING EN VERVOLGING IN CYBERSPACE

Masterproef van de opleiding
'Master in de rechten'

Ingediend door

Kevin Verhaeghe
(Studentennummer 00601047)

Promotor: Prof. Dr. Philip Traest
Commissaris: Tessa Gombeer

DANKWOORD

In dit dankwoord wil ik mij richten tot de mensen die mij de nodige hulp en steun verschaft hebben tijdens het schrijven van deze masterproef, en tijdens mijn rechtenstudies in het algemeen.

Vooreerst wens ik een dankwoord te richten tot Prof. Dr. Philip Traest, mijn promotor. Hij heeft mij te allen tijde met raad en daad bijgestaan. Zijn nuttige aanbevelingen hebben zonder twijfel een meerwaarde betekend voor dit werk.

Vervolgens wens ik ook mijn ouders, Jean-Marie Verhaeghe en Monique Verbuyst, uitdrukkelijk te bedanken. Zij hebben mij gedurende het schrijven van deze masterproef, en tijdens mijn rechtenstudies in het algemeen, steeds onvoorwaardelijk gesteund. Dit zowel op emotioneel, mentaal als financieel vlak. In het bijzonder wil ik mijn moeder bedanken voor het nauwgezet nalezen van dit werk.

Ook Luc Beirens verdient in dit kader een woord van dank. Hij maakte, ondanks zijn drukke agenda, tijd vrij om mijn vragen van een gepast antwoord te voorzien. Zijn inzichten zijn een grote bron van inspiratie geweest.

Tenslotte wens ik mijn vriendin Florence te bedanken. Haar steun, geduld en bemoedigende woorden maakten een wereld van verschil voor mij.

Kevin Verhaeghe

Humbeek, 15 mei 2012

INHOUDSTAFEL

DEEL I: INLEIDING EN PROBLEEMSTELLING 1

DEEL II: HET GEGEVEN CYBERSPACE 4

HOOFDSTUK 1: INLEIDING 5
HOOFDSTUK 2: DE GESCHIEDENIS VAN CYBERSPACE 5
HOOFDSTUK 3: INTERNETGEBRUIK IN BELGIË 7
1. INTERNETAANSLUITINGEN BELGISCHE HUISHOUDENS (NIS) 7
2. INTERNETAANSLUITINGEN BELGISCHE HUISHOUDENS (ISPA) 9
3. CONCLUSIE 11

DEEL III: CYBERCRIME, EEN SITUATIESCHETS 13

HOOFDSTUK 1: INLEIDING 14
HOOFDSTUK 2: CYBERCRIME 14
1. DE GESCHIEDENIS VAN CYBERCRIME 14
2. OMSCHRIJVING VAN HET CONCEPT CYBERCRIME 17
2.1 Definitie 17
2.2 Factoren die cybercrime in de hand werken 18
2.3 Constitutieve bestanddelen van cybercrime 19
2.3.1 Specifieke informaticacriminaliteit 21
2.3.1.1 Begrip 21
2.3.1.2 Computerinbraak 22
2.3.1.3 Manipulatie van elektronische gegevens 23
2.3.1.4 Illegaal kopiëren of verspreiden van computersoftware 24
2.3.1.5 Illegaal kopiëren van software 24
2.3.1.6 Illegaal kopiëren van muziek 24
2.3.1.7 Informaticabedrog 24
2.3.1.8 Valsheid in informatica 24
2.3.2 A-Specifieke informaticacriminaliteit 25
2.3.2.1 Begrip 25
2.3.2.2 Illegale verspreiding van pornografie 25
2.3.2.3 Bestraffing van de aanranding van de eer of de goede naam van personen 26
2.3.2.4 Bestraffing van racistische uitlatingen en ontkenning van de genocide 26
2.3.2.5 Aanzetten tot crimineel gedrag 26
2.3.2.6 Gokken 26
2.3.2.7 Oplichting 27
2.3.3 Recente categorisering 27
2.4 De nefaste gevolgen van cybercrime 29
3. EEN RECENTE VORM VAN CYBERCRIME: HET TOR-NETWERK 31
3.1 Inleiding 31
3.2 Wat is Tor? 31
3.3 Optreden tegen Tor? 33

DEEL IV: DE AANPAK VAN INTERNATIONALE ORGANISATIES INZAKE CYBERCRIMINALITEIT 35

HOOFDSTUK 1: INLEIDING 36
HOOFDSTUK 2: AANPAK VAN DE OESO 36
HOOFDSTUK 3: AANPAK VAN DE VN 37
HOOFDSTUK 4: AANPAK VAN DE G8 40
HOOFDSTUK 5: AANPAK VAN DE RAAD VAN EUROPA 45
1. INLEIDING 45
2. ONTSTAANSGESCHIEDENIS VAN HET CYBERCRIME-VERDRAG 47
3. BESPREKING VAN HET CYBERCRIME-VERDRAG 50
3.1 Doelstellingen 50

3.2 Summiere artikelsgewijze bespreking ... 51
3.2.1 Definities ... 52
3.2.2 Maatregelen op nationaal niveau ... 52
3.2.2.1 Materieel strafrecht ... 52
3.2.2.2 Strafprocesrecht ... 54
3.2.2.3 Rechtsmacht ... 56
3.2.3 Internationale samenwerking ... 56
3.2.3.1 Algemene beginselen van internationale samenwerking ... 56
3.2.3.2 Specifieke voorzieningen in het kader van internationale samenwerking ... 57
3.2.4 Slotbepalingen ... 58
3.3 Een kritische invalshoek ... 58
4. HET AANVULLEND PROTOCOL VAN 28 JANUARI 2003 ... 60
4.1 Algemeen ... 60
4.2 Bespreking van het protocol ... 61
4.2.1 Conceptueel kader ... 61
4.2.2 Definiëring ... 61
4.2.3 Nieuwe incriminaties ... 61
4.3 Een kritische invalshoek ... 63
HOOFDSTUK 6: AANPAK VAN DE EUROPESE UNIE ... 64
1. OVERZICHT VAN DE GENOMEN INITIATIEVEN ... 64
2. HET KADERBESLUIT 2005/222/JBZ VAN DE EUROPESE RAAD ... 68
2.1 Algemeen ... 68
2.2 Summiere artikelsgewijze bespreking ... 68
2.3 Richtlijn tot intrekking van Kaderbesluit 2005/222/JBZ ... 69
HOOFDSTUK 7: CONCLUSIE ... 71

DEEL V: DE BELGISCHE AANPAK INZAKE CYBERCRIMINALITEIT ... 73

HOOFDSTUK 1: INLEIDING ... 74
HOOFDSTUK 2: DE WET VAN 28 NOVEMBER 2000 INZAKE INFORMATICACRIMINALITEIT ... 74
1. DE STAND VAN ZAKEN VOORAFGAAND AAN DE WET ... 74
2. TOTSTANDKOMING VAN DE WET VAN 28 NOVEMBER 2000 INZAKE INFORMATICACRIMINALITEIT ... 75
3. BESPREKING VAN DE WET VAN 28 NOVEMBER 2000 INZAKE INFORMATICACRIMINALITEIT ... 76
3.1 Bepalingen tot aanvulling van het Strafwetboek ... 77
3.1.1 Valsheid in informatica (artikel 201bis Sw.) ... 77
3.1.2 Informaticabedrog (artikel 504quater Sw.) ... 77
3.1.3 Ongeoorloofde toegang (artikel 550bis Sw.) ... 78
3.1.4 Informaticasabotage (artikel 550ter Sw.) ... 80
3.1.5 Conclusie ... 80
3.2 Bepalingen tot wijziging van het Wetboek van Strafvordering ... 82
3.2.1 Databeslag (artikel 39bis Sv.) ... 82
3.2.2 Netwerkzoeking (artikel 88ter Sv.) ... 83
3.2.3 Medewerkingsverplichting (artikel 88quater Sv.) ... 85
3.2.4 Aanvullingen van de artikelen 90ter, 90quater en 90septies Sv. ... 86
3.3 Nieuwe bepalingen in de Belgacomwet ... 87
3.4 Wijzigingen van de wet van 28 november 2000 inzake informaticacriminaliteit ... 90
4. DE BESTRAFFING VAN VERWANTE MISDRIJVEN ... 92
4.1 Inleiding ... 92
4.2 Aanranding van de eer of de goede naam ... 92
4.3 Gokken op het internet ... 92
4.4 Oplichting ... 93
5. EVALUATIE VAN DE WET VAN 28 NOVEMBER 2000 INZAKE INFORMATICACRIMINALITEIT ... 93
HOOFDSTUK 3: IMPLICATIES VAN HET CYBERCRIME-VERDRAG OP HET VOORONDERZOEK ... 94
1. INLEIDING ... 94
2. HET VASTLEGGINGSBEVEL ... 94
3. HET OVERLEGGINGSBEVEL ... 96
4. DE NETWERKZOEKING EN INBESLAGNAME ... 97

5. DE INTERNATIONALE NETWERKZOEKING 98
HOOFDSTUK 4: DE OPSPORING VAN CYBERCRIMINALITEIT IN BELGIË 99
1. INLEIDING 99
2. DE BELGISCHE OPSPORINGSINSTANTIES 99
2.1 Algemeen kader 99
2.2 Regional Computer Crime Units (RCCU) 100
2.3 Federal Computer Crime Unit (FCCU) 101
2.3.1 Organisatie 101
2.3.2 Strategische doelstellingen 102
2.3.3 Activiteitsdomeinen 103
2.3.4 Budget 105
2.3.5 Personeel 106
2.3.6 Samenwerking met niet-politionele diensten 106
2.3.6.1 ISPA 106
2.3.6.2 CERT 107
2.3.6.3 BIPT 107
2.3.6.4 Spamsquad-werkgroep 108
2.3.6.5 BelNIS-werkgroep 108
2.3.7 De FCCU en de opsporing 108
2.3.8 Enkele resultaten 109
2.3.9 De FCCU op de weegschaal 111
3. KRITISCHE BESCHOUWINGEN 113
3.1 Het wettelijk kader 113
3.2 Het verdere verloop na de opsporing 114
3.3 Het publieke bewustzijn 115
3.4 Bemerking omtrent het personeel en het budget 115
3.5 Gebrek aan een Koninklijk Besluit inzake dataretentie 116
3.6 De hoeveelheid aangiftes 117
HOOFDSTUK 5: DE VERVOLGING VAN CYBERCRIMINALITEIT IN BELGIË 117
1. INLEIDING 117
2. OMZENDBRIEVEN VAN HET COLLEGE VAN PROCUREURS-GENERAAL 119
2.1 Omzendbrieven met betrekking tot de aanpak van verschijningsvormen van cybercriminaliteit 119
2.1.1 Omzendbrief COL 13 van 1 oktober 1998 119
2.1.2 Omzendbrief COL 12 van 3 juni 1999 119
2.1.3 Omzendbrief COL 1 van 14 februari 2002 120
2.1.4 Omzendbrief COL 8 van 9 april 2004 121
2.1.5 Omzendbrief COL 6 van 21 maart 2006 122
2.1.6 Omzendbrief COL 2 van 19 februari 2009 122
2.1.7 Omzendbrief COL 14 van 17 december 2009 123
2.2 Omzendbrieven met betrekking tot de internationale samenwerking 124
2.3 Omzendbrieven met betrekking tot de werking van de FCCU 125
2.3.1 Omzendbrief COL 2 van 7 maart 2002 125
2.3.2 Omzendbrief COL 9 van 18 juni 2009 125
3. STATISTISCHE GEGEVENS OMTRENT DE VERVOLGING 126
3.1 Inleiding 126
3.2 Instroom van zaken met betrekking tot de tenlastelegging ‘informatica’ 127
3.3 Hangende zaken met betrekking tot de tenlastelegging ‘informatica’ 128
3.4 Uitstroom van zaken met betrekking tot de tenlastelegging ‘informatica’ 128
HOOFDSTUK 6: DE STRAFTOEMETING DOOR DE RECHTER 130
1. INLEIDING 130
2. BESPREKING VAN DE RELEVANTE RECHTSPRAAK 131
2.1 Vonnis van 15 december 2003 van de correctionele rechtbank te Eupen 131
2.2 Vonnis van 28 november 2005 van de correctionele rechtbank te Dendermonde 131
2.3 Vonnis van 29 augustus 2008 van de rechtbank van eerste aanleg te Dendermonde’ 132
2.4 Vonnis van 14 november 2008 van de rechtbank van eerste aanleg te Dendermonde’ 133
2.5 Vonnis van 14 mei 2007 van de correctionele rechtbank te Dendermonde’ 134
2.6 Arrest van 10 september 2008 van het hof van beroep te Antwerpen 134

2.7 Vonnis van 8 januari 2008 van de correctionele rechtbank te Brussel ... 135
2.8 Vonnis van 21 januari 2004 van de correctionele rechtbank te Hasselt ... 135
2.9 Vonnis van 10 januari 2008 van de correctionele rechtbank te Brussel ... 136
2.10 Arrest van 7 oktober 2003 van het hof van beroep te Antwerpen ... 136
2.11 Vonnis van 2 augustus 2009 van de correctionele rechtbank te Dendermonde' ... 137
3. CONCLUSIE ... 137
HOOFDSTUK 7: CONCLUSIE ... 137

DEEL VI: DE NEDERLANDSE AANPAK INZAKE CYBERCRIMINALITEIT ... 139

HOOFDSTUK 1: INLEIDING ... 140
HOOFDSTUK 2: HET WETTELIJK KADER ... 140
1. MATERIEEL STRAFRECHT ... 140
1.1 Binnendringen in een geautomatiseerd werk ... 142
1.2 Stoornis in de gang of werking van een geautomatiseerd werk ... 142
1.3 Onbruikbaar maken, veranderen of aantasten van gegevens ... 143
1.4 Afluisteren ... 144
2. STRAFPROCESRECHT ... 144
3. CONCLUSIE ... 145
HOOFDSTUK 3: DE OPSPORING EN VERVOLGING VAN CYBERCRIMINALITEIT IN NEDERLAND ... 146
1. DE GEÏNTEGREERDE SAMENWERKING ... 146
2. DE OPSPORINGSINSTANTIES ... 147
2.1 Korps Landelijke Politiediensten ... 147
2.2 Nationaal Team High Tech Crime ... 147
2.3 Team Bestrijding Kinderporno en Kindersekstoerisme ... 148
3. DE VERVOLGING ... 148
4. ANDERE INSTELLINGEN ... 149
4.1 Govcert.nl ... 149
4.2 Nationaal Cyber Security Centrum ... 149
5. DE AANPAK VAN BREDOLAB: EEN SUCCESVERHAAL ... 149
HOOFDSTUK 4: DE STRAFTOEMETING DOOR DE RECHTER ... 150
1. BESPREKING VAN DE RELEVANTE RECHTSPRAAK ... 150
1.1 Arrest van 21 november 2006 van het Gerechtshof te Arnhem ... 150
1.2 Vonnis van 8 december 2010 van de rechtbank van eerste aanleg te Utrecht ... 151
1.3 Arrest van 23 maart 2012 van het Gerechtshof te 's-Gravenhage ... 151
2. CONCLUSIE ... 151
HOOFDSTUK 5: CONCLUSIE ... 152

DEEL VII: DE AANPAK VAN DE VERENIGDE STATEN INZAKE CYBERCRIMINALITEIT ... 153

HOOFDSTUK 1: INLEIDING ... 154
HOOFDSTUK 2: HET WETTELIJK KADER ... 154
1. MATERIEELRECHTELIJKE BEPALINGEN ... 154
1.1 The Computer Fraud and Abuse Act ... 154
1.2 The Child Pornography Protection Act ... 155
1.3 The Wiretap Act ... 155
1.4 The Electronic Communications Privacy Act ... 156
2. BEPALINGEN VAN STRAFPROCESRECHT ... 156
3. CONCLUSIE ... 156
HOOFDSTUK 3: DE OPSPORING EN DE VERVOLGING IN DE VERENIGDE STATEN ... 157
1. INLEIDING ... 157
2. DE OPSPORINGSINSTANTIES ... 157
2.1 Federal Bureau of Investigation (FBI) ... 157
2.1.1 Algemeen ... 157
2.1.2 Carnivore ... 158
2.2 United States Secret Service ... 158
2.3 Homeland Security ... 159

3. De vervolging van cybercriminaliteit 159
4. Conclusie 159
Hoofdstuk 4: De straftoemeting door de rechter 160
1. Inleiding 160
2. US vs. Jason Arabo 160
3. US vs. Kenneth Kwak 161
4. US vs. jeanson James Anceta 161
5. US vs. kenneth Flury 161
6. Conclusie 161
Hoofdstuk 5: Conclusie 162
DEEL VIII: ALGEMENE CONCLUSIE 163
DEEL IX: BIBLIOGRAFIE 170
DEEL X: BIJLAGEN 191

DEEL I: Inleiding en probleemstelling

1. Mijn keuze voor het onderwerp ‘Opsporing en vervolging in cyberspace’ is grotendeels gesteund op twee redenen. Vooreerst heb ik steeds een uitgesproken interesse gehad voor alles wat met strafvordering te maken heeft. Vervolgens ben ik, zoals zoveel mensen van mijn generatie, in zekere zin verknocht aan het internet.

2. De laatste twee decennia heeft onze samenleving een ware digitale revolutie ondergaan. Het gebruik van ICT is een doodnormale zaak geworden. De technologische vooruitgang heeft tal van voordelen opgeleverd, op zowat alle vlakken van de maatschappij. Het internet heeft zich doorheen de jaren in de harten van de bevolking genesteld. Het merendeel van de bevolking beschouwt het internet dan ook als een nuttig iets. Het wordt aanzien als zijnde een betrouwbaar en veilig medium, met een hoge graad van anonimiteit. Deze mate van anonimiteit, die lager ligt dan vele mensen geloven, trekt echter ook personen met minder goede bedoelingen aan. Criminaliteit begint zich dan ook hoe langer hoe meer te manifesteren in deze virtuele wereld. Deze transitie brengt voor de opsporings- en vervolgingsinstanties aanzienlijke problemen met zich mee. Ook het wetgevend kader dient in dat opzicht aangepast te worden. Bij het schrijven van deze masterproef ben ik nagegaan op welke wijze de opsporing en vervolging van cybercriminaliteit concreet verloopt, en op welke manier men de voorafgaande problemen al dan niet heeft proberen aan te pakken. De nadruk in dit werk ligt op de Belgische situatie. Toch ben ik ook over de landsgrenzen heen gaan kijken. Meer bepaald heb ik, zij het op een summiere wijze, de gang van zaken in Nederland en in de Verenigde Staten besproken. Op deze wijze kan men de situatie in België spiegelen aan twee andere landen, wat kan leiden tot verhelderende inzichten. De concrete opbouw en structuur van mijn masterproef, licht ik u in de hierop volgende paragrafen toe.

3. Deel II is volkomen gewijd aan het internet, in academische middens ook wel ‘cyberspace’ genoemd. In dit deel wordt er een overzicht gegeven van de ontstaansgeschiedenis van het internet. Tevens tracht ik een beeld te scheppen omtrent de plaats die het internet in onze samenleving inneemt. Dit geschiedt aan de hand van statistische cijfers van het Nationaal Instituut voor de Statistiek, en de Internet Service Providers Association.

4. In deel III wordt het fenomeen ‘cybercrime’ besproken. Er wordt meer bepaald ingegaan op de geschiedenis van cybercrime, welke criminaliteitsvormen er juist onder cybercrime dienen te worden verstaan, en welke schade cybercrime veroorzaakt.

5. Deel IV is gewijd aan de internationale organisaties die initiatieven hebben genomen in de strijd tegen cybercriminaliteit. In dit deel wordt er uitgebreid aandacht besteed aan het Cybercrime-Verdrag van de Raad van Europa, gezien dit tot op vandaag het enige internationale verdrag is met betrekking tot de aanpak van cybercrime. Naast de Raad van Europa, wordt ook de OESO, de VN, de G8, en de EU besproken.

6. In deel V licht ik de Belgische situatie toe. De wet van 28 november 2000 neemt hier een sleutelpositie in. Aan deze wet wordt dan ook de nodige aandacht besteed, zowel wat de strafbaarstellingen, als de bepalingen van strafprocesrecht betreft. Naast dit wetgevend kader wordt ook de opsporing van cybercriminaliteit in België besproken. Aan de Federal Computer Crime Unit is dan ook een apart hoofdstuk gewijd. Wat de vervolging betreft, wordt de situatie van de parketten bij de rechtbanken van eerste aanleg besproken. Aan de hand van statistisch materiaal wordt weergegeven in welke mate de verschillende parketten cybercriminaliteit vervolgen. Tenslotte wordt de theorie getoetst aan de praktijk, waarbij enkele relevante vonnissen en arresten worden besproken.

7. Deel VI schetst de Nederlandse aanpak inzake cybercriminaliteit. Naast een overzicht van het wettelijk kader, worden ook de relevante opsporingsdiensten besproken. Verder wordt er ook aandacht geschonken aan de vervolging en de straftoemeting.

8. Deel VII heeft betrekking op de aanpak van cybercriminaliteit in de Verenigde Staten. Ook hier worden de hoofdlijnen van het wettelijk kader besproken, evenals de betrokken opsporingsdiensten. Naast deze punten wordt er tevens aandacht besteed aan de wijze waarop de vervolging in de VS verloopt, en worden enkele zaken uit de praktijk van naderbij bekeken.

9. Deel VIII omvat de algemene conclusie van dit werk. Hier worden mijn bevindingen omtrent de opsporing en vervolging in cyberspace op een kritische wijze weergegeven.

DEEL II: Het gegeven cyberspace

Hoofdstuk 1: Inleiding

10. Om een volledig beeld te kunnen krijgen over de opsporing en vervolging in cyberspace is het opportuun om eerst en vooral stil te staan bij het gegeven 'cyberspace'. Dit deel zal dan ook het concept cyberspace nader toelichten. Eerst en vooral zal de geschiedenis van het internet behandeld worden, gevolgd door een weergave van het hedendaagse gebruik van het internet in België.

Hoofdstuk 2: De geschiedenis van cyberspace

11. Cyberspace is een term die voor het eerste werd gebruikt door William Gibson, in zijn boek Neuromancer.[1] Op deze manier kreeg de term bekendheid, waarna het in de jaren '90 uitgroeide tot een synoniem voor het World Wide Web. Evenwel zag het internet al veel vroeger het levenslicht.

12. In 1962, ten tijde van de Koude Oorlog, schreef Paul Baran een rapport voor de Rand Corporation aangaande de bescherming van Amerikaanse communicatiesystemen. Meer bepaald ging hij na hoe de Verenigde Staten haar communicatielijnen zou kunnen beschermen tegen militaire acties van de toenmalige USSR. [2] Paul Baran stelde vast dat de communicatiesystemen van de Verenigde Staten op dat moment zeer kwetsbaar waren. Hij poogde dit oud zeer te verhelpen door gebruik te maken van een systeem waar geen herkenbaar centraal commando- en controlepunt bestaat. Op deze manier zou een aanval op het systeem niet leiden tot een volledige break-down.[3] Schade aan een bepaald onderdeel kan immers het geheel niet vernietigen, waardoor het effect aanzienlijk wordt gereduceerd. Met de hulp van de University of California, staat Paul Baran in september 1969 aan de wieg van een compleet nieuw systeem. Op dat tijdstip werd namelijk de eerste Arpanet Information Message Processor bij de UCLA geïnstalleerd.[4] [5] Het Arpanet was een mijlpaal, een voorloper die als basis diende voor het internet zoals wij het vandaag kennen.

[1] W. GIBSON, *Neuromancer*, Vancouver, Harper Collins Paperback, 1995.
[2] M. KÖHLER en ARNDT, *Recht des Internet*, Heidelberg, Müller Verlag, 2000, 2-3.
[3] K. HAFNER en M. LYON, *Where wizards stay up late : The origins of the internet*, New York, Simon & Schuster, 1998, 12.
[4] M. YAR, *Cybercrime and society*, Londen, Sage Publications ltd, 2006, 7.
[5] UCLA staat voor University of California, Los Angeles.

13. De kracht van het Arpanet zat in het principe van de 'dynamic routering'.[6] Dynamic routering is een systeem waarbij een gedecentraliseerde netwerkstructuur op poten wordt gezet, zodat bij een eventuele onderbreking van een verbinding de informatie-uitwisseling automatisch via een andere weg verloopt. Arpanet was op dat moment een louter militair verhaal. Het werd gesubsidieerd door het programma voor 'Advance Research Projects Agency' van het Amerikaanse ministerie van Defensie. Op militair vlak was het Arpanet een succesverhaal, in die mate dat het in 1972 werd uitgebreid voor wetenschappelijke en universitaire doeleinden. Nog geen jaar later werden er internationale verbindingen gelegd, zodat informatie-uitwisseling niet meer aan landsgrenzen gebonden was.

14. In 1977 omvatte het Arpanet al meer dan vijftig sites.[7] Het ontwikkelen van Arpanet was zonder enige twijfel een huzarenstukje van formaat. Maar ondanks de belangrijke invloed kampte Arpanet met enkele significante nadelen. Zo was de toegang tot Arpanet beperkt tot universiteiten die overeenkomsten hadden met het Amerikaanse ministerie van Defensie. Begin jaren '80 kwam hier verandering in. Enkele informaticastudenten ontwierpen een netwerk dat open was voor iedereen. Op deze manier ontstond 'A poor man's Arpanet'[8], Usenet News genaamd. Gelijktijdig werd er met 'IP'[9] een universele taal ontwikkeld, die het mogelijk maakte dat computers over de hele wereld met elkaar in verbinding staan.[10] Aparte netwerken konden op deze wijze met elkaar in verbinding staan door gebruik te maken van dit IP-protocol.[11]

15. Tegenwoordig klinkt cyberspace ons meer bekend in de oren in de vorm van de toepassing 'World Wide Web'.[12] Het WWW werd ontwikkeld in Zwitserland, aan het Europees Instituut voor Deeltjesfysica (CERN). De taak van de ontwikkeling en uitbouw was in se geen taak voor het CERN. In 1994 werd dan ook een afzonderlijk instituut opgericht om hierop toe te zien, het World Wide Web Consortium (W3C).[13] Het World Wide Web is gesteund op HTML[14], een programma dat het mogelijk maakt om webpagina's te voorzien

[6] M. YAR, *Cybercrime and society*, Londen, Sage Publications ltd, 2006, 7.
[7] B. STERLING, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Harmondsworth, Penguin, 1994, 15.
[8] https://w2.eff.org/Net_culture/net.history.txt.
[9] IP staat voor Internet Protocol.
[10] K. HAFNER en M. LYON, *Where wizards stay up late : The origins of the internet*, New York, Simon & Schuster, 1998, 15.
[11] M. KÖHLER en ARNDT, *Recht des Internet*, Heidelberg, Müller Verlag, 2000, 4.
[12] M. YAR, *Cybercrime and society*, Londen, Sage Publications ltd, 2006, 7.
[13] www.w3.org.
[14] HTML staat voor HyperText Markup Language.

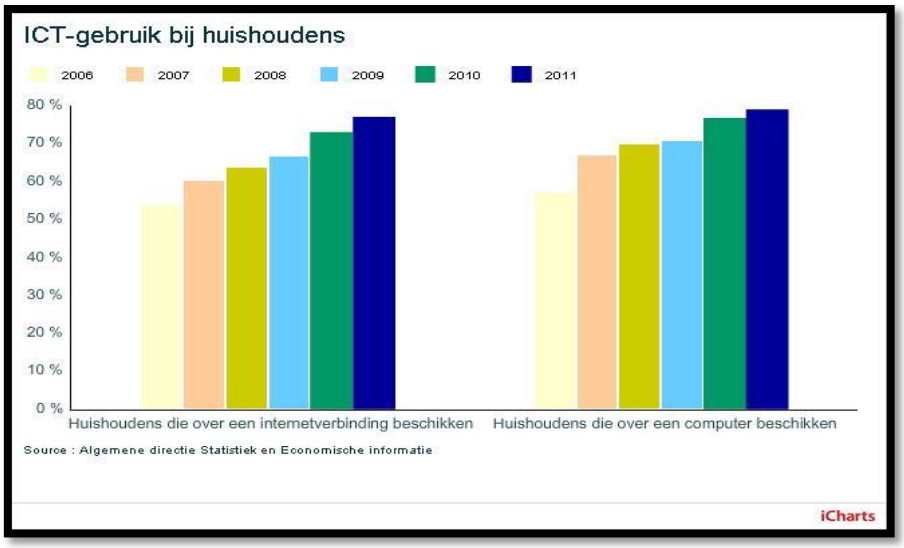
van tekst, afbeeldingen e.d.. Webpagina's kunnen worden bekeken via een browser, zoals Internet Explorer (Microsoft) of Firefox.[15] [16]

Hoofdstuk 3: Internetgebruik in België

1. INTERNETAANSLUITINGEN BELGISCHE HUISHOUDENS (NIS)

16. Het internetgebruik in België is, als we naar de cijfers van het Nationaal Instituut voor de Statistiek (NIS) kijken, het laatste decennium aan een markante opmars bezig. Dit vormt een mooi bewijs dat de computer al enige tijd gemeengoed is in het doorsnee Belgische huishouden. In 2005 had 50% van de Belgische huishoudens toegang tot het internet. In 2011 is dit aantal al gestegen tot 73%, een forse toename van maar liefst 23%.[17]

FIGUUR 1: EVOLUTIE VAN HET ICT-GEBRUIK BIJ HUISHOUDENS GEDURENDE DE PERIODE 2006-2011

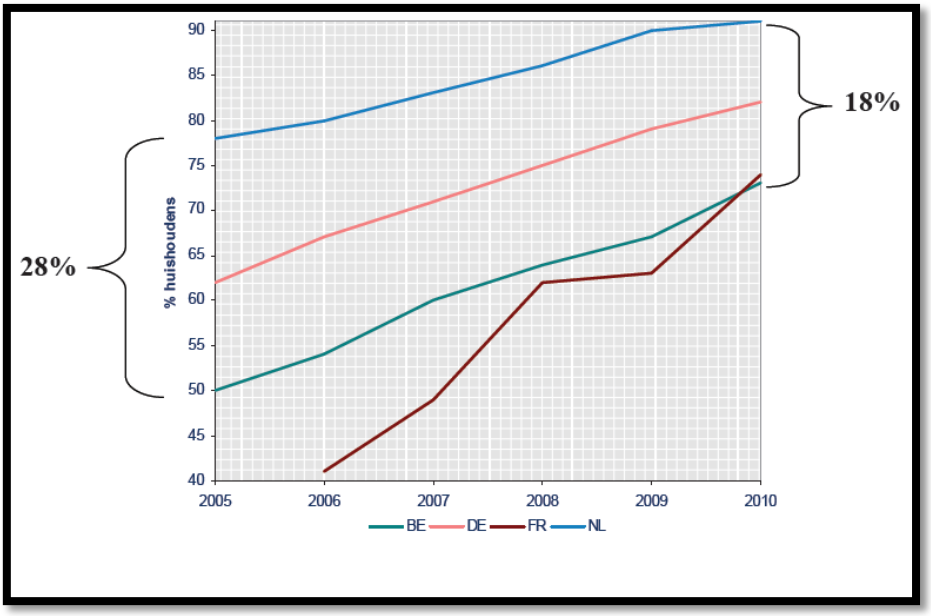


17. België volgt met dit cijfer Frankrijk op de voet (76%), maar heeft wel nog een significante achterstand op landen als Duitsland (86%) en Nederland (92%). Europees gezien bevindt België zich in dit kader op het gemiddelde van de EU. Nederland is in dit opzicht zelfs de beste leerling in de Europese klas. Niettemin wordt de achterstand van België ten

[15] M. YAR, *Cybercrime and society*, Londen, Sage Publications ltd, 2006, 8.
[16] K. HAFNER en M. LYON, *Where wizards stay up late : The origins of the internet*, New York, Simon & Schuster, 1998, 12.
[17] http://statbel.fgov.be/nl/statistieken/cijfers/arbeid_leven/ict/.

opzichte van Nederland steeds kleiner en kleiner. Zo is het verschil sinds het jaar 2005 gedaald van 28 naar 18%.[18] Er is dus wel degelijk sprake van een digitale revolutie, een opmars van het gebruik van het internet.

FIGUUR 2: EVOLUTIE VAN HET PERCENTAGE HUISHOUDENS MET TOEGANG TOT INTERNET THUIS OVER DE PERIODE 2005-2010. VERGELIJKING VAN BELGIË MET DE BELANGRIJKSTE BUURLANDEN



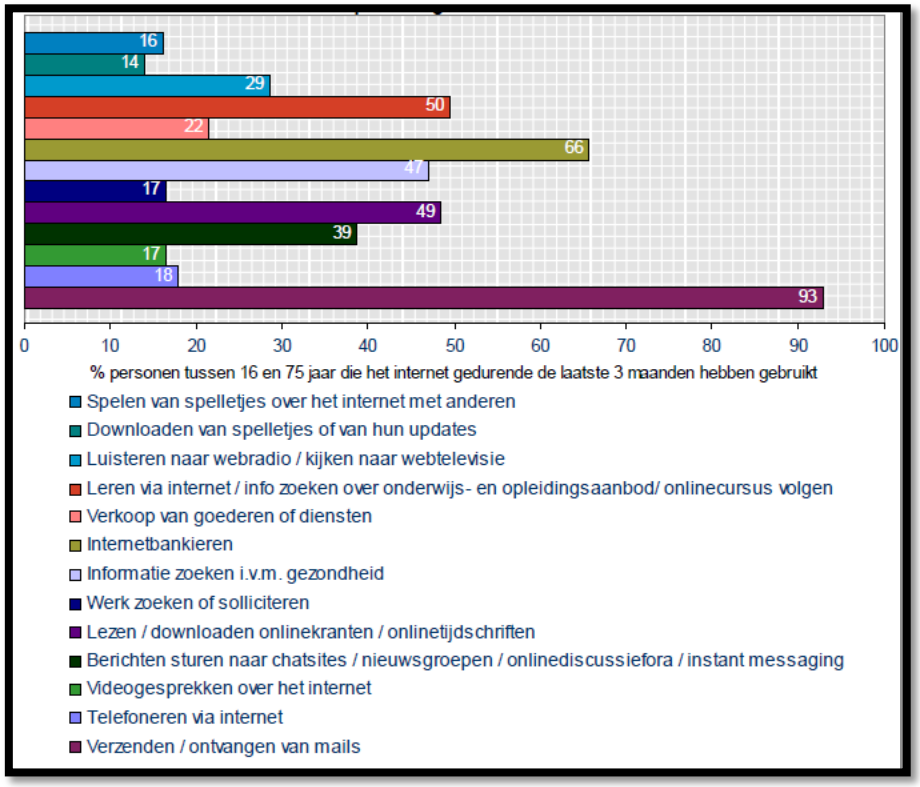
18. We dienen hieromtrent wel een onderscheid te maken tussen het toegang hebben tot het internet en het effectief gebruik van het internet, om welke reden dan ook. Niettemin valt uit de cijfers van het NIS wel af te leiden dat de meeste Belgen die effectief internet gebruiken, dat ook veel doen. Maar liefst 77% van de ondervraagde personen gebruikte in de drie maanden voorafgaand aan de enquête het internet dagelijks, 19% van diezelfde personen gebruikt het internet wekelijks. Een kleine restgroep gebruikt het internet op minder frequente basis.

19. De gemiddelde Belg gebruikt het internet voor een veelheid van toepassingen. Uit onderstaande tabel blijkt dat het verzenden en ontvangen van e-mails met voorsprong de belangrijkste activiteit van de internet gebruikende Belg blijft (93%).[19] Hieruit blijkt eens te meer hoe onze sociale interactie en manier van communicatie is gewijzigd, en dat op een

[18] Nationaal Instituut voor de Statistiek, *Digitale (r)evolutie in België –anno 2010* (persbericht), Brussel, 2011, http://statbel.fgov.be/nl/binaries/ict2010-nl_tcm325-117754.pdf, 1.
[19] Nationaal Instituut voor de Statistiek, *Digitale (r)evolutie in België –anno 2010* (persbericht), Brussel, 2011, http://statbel.fgov.be/nl/binaries/ict2010-nl_tcm325-117754.pdf, 2.

relatief kort tijdsbestek. Het meer veralgemeend gebruik van het internet vond immers amper een kleine twintig jaar geleden zijn ingang. Een andere belangrijke en wijd verspreide activiteit op het internet is die van het internetbankieren. Maar liefst 66% van de ondervraagde personen handelt immers zijn bankzaken via het internet af. Minder populaire activiteiten zijn het telefoneren of het voeren van videogesprekken over het internet.[20]

FIGUUR 3: PERCENTAGES VAN DE ACTIVITEITEN UITGEVOERD OP INTERNET IN 2010



2. INTERNETAANSLUITINGEN BELGISCHE HUISHOUDENS (ISPA)

20. Een andere instantie die zich bezighoudt met het nagaan van de evolutie van private internetaansluitingen is de Belgian Internet Service Providers Association, afgekort ISPA..[21] De ISPA werd opgericht in 1997 en omvat de meerderheid van Belgische internetaanbieders. Zo zijn bijvoorbeeld Telenet, Belgacom, Scarlet en Mobistar lid van de ISPA. De ISPA is een vereniging zonder winstoogmerk die erop gericht is om, in algemene bewoordingen, de groei van het internet en aanverwante diensten te bevorderen evenals de belangen van

[20] Nationaal Instituut voor de Statistiek, *Digitale (r)evolutie in België –anno 2010* (persbericht), Brussel, 2011, http://statbel.fgov.be/nl/binaries/ict2010-nl_tcm325-117754.pdf, 2.
[21] www.ispa.be.

internetproviders te behartigen. Meer specifiek richten ze zich op een viertal activiteiten. Vooreerst biedt de ISPA een forum voor de overheid en andere organisaties met het oog op discussies omtrent de relevantie van de internetindustrie. De ISPA stelt zich eveneens tot doel relevante informatie omtrent het internet in België ter beschikking te stellen. Een andere verwezenlijking van de ISPA bestaat erin dat ze een algemene Code of Conduct heeft gecreëerd voor de Belgische internetproviders. Tenslotte staan zij ook in voor communicatie met gelieerde organisaties, zowel in België als wereldwijd.

21. Elk kwartaal doet de ISPA een marktonderzoek naar het aantal particuliere internetaansluitingen in België. Het meest recente marktonderzoek dateert van het vierde kwartaal van het jaar 2011. Uit deze market survey (N°50) blijkt dat het aantal actieve, particuliere internetaansluitingen gestaag blijft stijgen. [22] Het totaal aantal actieve verbindingen bedraagt momenteel 3.481.767, een stijging van 0,96% ten opzichte van het derde kwartaal van 2011. Het grootste deel van dat aantal is particulier, met name 2.833.714. De overige 648.053 verbindingen situeren zich in het ondernemingsleven.[23] Waar het aantal actieve internetverbindingen begin deze eeuw nog rond 300.000 schommelden, kunnen we zeggen dat dit aantal in twaalf jaar tijd enorm is toegenomen.

22. Naast het bijhouden van het aantal actieve verbindingen is er nog een degelijke parameter om het internetgebruik in kaart te brengen. De ISPA houdt meer bepaald eveneens het aantal geregistreerde domeinnamen in België bij. Initieel was het professor Verbaeten (KUL) die zich toelegde op de registratie van domeinnamen. De ISPA nam na verloop van tijd, in het jaar 1999, deze taak over en installeerde een werkgroep, bestaande uit de ISPA, Agoria en Beltug. Op deze manier zag DNS Belgium het licht.[24] De vereniging houdt zich bezig met de organisatie van de registratie van domeinnamen, en staat tevens in voor de continuïteit van diezelfde domeinnamen. Meer concreet zijn de taken van DNS Belgium de volgende: [25]

- het uitwerken van het beleid en van de procedures betreffende de registratie, evenals het opstellen van de regels en voorschriften;
- het garanderen van de kwaliteit van de registratie van de domeinnamen in België;
- het beheren en organiseren van alle technische aspecten van de registratie;
- het sluiten van overeenkomsten met de registrars;

[22] Internet Services Providers Association, *Market Survey N°50 - Q4 2011*, Brussel, 2012, www.ispa.be.
[23] Internet Services Providers Association, *Market Survey N°50 - Q4 2011*, Brussel, 2012, www.ispa.be.
[24] DNS staat voor Domain Name System.
[25] www.ispa.be.

- het op nationaal niveau coördineren van de registratie van de namen;
- het vertegenwoordigen van '.be' bij internationale regulerende instanties en werkgroepen;
- het opvolgen van de technologische evolutie in het kader van de domeinnamen;
- het stimuleren van de standaardisatie;
- het stimuleren van de samenwerking tussen de Internet Service Providers.

23. DNS Belgium komt net als het NIS en de ISPA tot de conclusie dat het internetgebruik in België sinds het laatste decennium aan een sterke opmars bezig is. Het aantal geregistreerde domeinnamen, zoals bijgehouden door DNS Belgium, spreekt in dit kader boekdelen. Tot in 1994 werden er 129 domeinnamen geregistreerd, een peulschil vergeleken met het huidige aantal. Toen DNS Belgium rond de eeuwwisseling werd opgericht, gold er een zeer rigide regime met betrekking tot het verkrijgen van een domeinnaam. Enkel bedrijven konden op dat punt een domeinnaam laten registreren, verder dienden strikte formaliteiten te worden nageleefd. Eind 2000 werd het systeem drastisch vereenvoudigd, de hele procedure werd veel flexibeler gemaakt. Er werd overgegaan tot een volledige liberalisering van het systeem, met als gevolg dat elke Belg of buitenlander, privaat of professioneel, een domeinnaam kon laten registreren. De formaliteiten vielen grotendeels weg, en de registratie verliep van dan af automatisch. Parallel met deze vereenvoudiging kwam er ook een grote prijsdaling. Dit alles had tot gevolg dat het aantal geregistreerde domeinnamen pijlsnel omhoogschoot. Bij de start van de liberalisering in het jaar 2000, waren er ongeveer 40.000 geregistreerde domeinnamen. Nog geen drie weken later was dat aantal al verdubbeld. Jaar na jaar is dat aantal substantieel blijven toenemen. De huidige stand van zaken is verbluffend, begin 2012 staat de teller immers op 1.266.709.[26]

3. CONCLUSIE

24. Uit bovenstaande gegevens blijkt duidelijk dat onze samenleving het afgelopen decennium een subtiele digitale revolutie heeft ondergaan, het internet neemt hoe langer hoe meer een belangrijke positie in ons leven in. Niet alleen in België, ook op het Europese niveau zien we een snel stijgende tendens. Internet op zich is een relatief nieuw fenomeen, waardoor de evolutie ervan naar de toekomst toe moeilijk in te schatten valt. Wat echter wel vaststaat, is

[26] www.ispa.be.

dat digitalisering de toekomst is, en dat het internet daarin een belangrijke rol zal blijven spelen. Zo zien we dat de laatste jaren smartphones een prominente rol beginnen op te eisen, een nieuwe invulling van het concept.

25. De voordelen van dit medium zijn zonder enige twijfel eindeloos. Enerzijds, is dit de grote kracht van een medium als internet. Anderzijds, kan het ook een achilleshiel betekenen. De vraag is immers hoe de hedendaagse maatschappij omgaat, en zal omgaan, met de minder fraaie kantjes van het internet. De uitdaging om misbruiken via dit medium tegen te gaan zal een enorme uitdaging vormen voor onze politiediensten. Het is voor een overheid, en meer specifiek voor politiediensten, sowieso al moeilijk om steeds mee te zijn met nieuwe ontwikkelingen. Het reguleren van een fenomeen als internet, dat in elk opzicht razendsnel verandert, is in dat opzicht dan ook geen sinecure.

DEEL III: Cybercrime, een situatieschets

Hoofdstuk 1: Inleiding

26. Het internet krijgt sinds enige tijd een steeds prominentere rol in ons leven. Sociale media als Facebook, Twitter en dergelijke meer zijn niet meer uit het dagelijkse leven weg te denken. De vrijheid en ongebreideldheid die cyberspace elk individu aanbiedt, en waar deze laatste dankbaar gebruik van maakt, heeft echter ook een schaduwkant. Misdrijven, zoals we die voordien enkel in de realiteit zagen, maken hun transitie naar deze virtuele wereld, met alle gevolgen van dien.

Hoofdstuk 2: Cybercrime

1. DE GESCHIEDENIS VAN CYBERCRIME

27. Het opkomen van de digitale technologie heeft een grote impact op eenieders leven. Ondanks het onnoemelijk aantal voordelen is er echter ook een donkere kant aan dit verhaal. Misdaad gaat namelijk hand in hand met opportuniteiten, dat is een gegeven van alle tijden. Onze groeiende afhankelijkheid van computers en de daarbij horende technologie biedt dergelijke opportuniteiten.

28. Het idee om computercriminaliteit te beschouwen als een separate categorie in het misdrijfspectrum is niets nieuws. Het idee werd voor het eerst geopperd in de jaren ’60 en ’70, gelijklopend met de opkomst van computers.[27] Toen al werd er gewag gemaakt van delicten als computersabotage en spionage. Computers speelden in die tijd echter nog geen wezenlijke rol in het dagelijkse leven, waardoor de aandacht ervoor relatief beperkt bleef. Naarmate de jaren ’70 voorbijgaan zien we echter dat er meer empirisch onderzoek wordt gedaan naar het fenomeen.[28] Hierop volgend zien we dat er nieuwe wetten het daglicht zien, specifiek gericht op het bestrijden van computercriminaliteit. In eerste instantie waren deze erop gericht te vermijden dat er wordt ingebroken in een systeem met het oog om privé informatie te verkrijgen. Later kwam hier ook een economische component bij.

[27] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 3.
[28] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 4.

29. Begin de jaren '80 ontstond het besef dat cybercrime een reëel probleem is.[29] De grote uitdaging om cybercrime aan te pakken, zit hem niet zozeer in de misdrijven zelf, wel in de vluchtigheid en uitgestrektheid van het medium waar ze plaatsvinden. Cybercrime stopt immers niet aan de landsgrenzen, het is een globaal probleem. In dat opzicht hebben tal van internationale organisaties zich over dit vraagstuk gebogen. Zowel de Verenigde Naties, de G8, Interpol als de Raad van Europa stelden richtlijnen op om zich te wapenen tegen het fenomeen.[30] [31]Gezien het globale karakter van cybercrime dringt zich een geharmoniseerde aanpak op. Een grotere vorm van harmonisatie kan de uitwisseling van informatie en de effectieve aanpak enigszins vergemakkelijken. Een vorm van dubbele discriminatie zou in dit opzicht bijvoorbeeld zeer welkom zijn. Niettemin is het ietwat naïef om in dit kader een algemene consensus te verwachten. Landen zijn, deels om begrijpelijke redenen, gesteld op hun soevereiniteit wat betreft het opleggen van standaarden met betrekking tot het strafrecht. Men kan eveneens niet uitsluiten dat bepaalde landen zich zouden willen profileren als zogezegde veilige havens, waar de regelgeving veel minder stringent is. Voor andere landen, zoals derdewereldlanden, is cybercrime ook verre van een prioriteit.[32] Wat men wel kan nastreven is een soort van breed gedragen consensus, een basis om op verder te bouwen in de toekomst. Hierop is het Cybercrime-Verdrag van de Raad van Europa gesteund, het eerste en tot nog toe enige multilaterale instrument in de strijd tegen cybercriminaliteit.[33]

30. Wat België betreft, was de Bistel-zaak[34] [35]een eerste harde confrontatie met cybercrime. In deze zaak werd, voor het eerst in België, computerinbraak bestraft.[36] [37]Centraal in deze zaak staat het informatiesysteem BISTEL, afkorting voor het Belgian Information System By Telephone. BISTEL is een elektronisch informaticasysteem dat, enerzijds, toegang verschaft tot databanken en, anderzijds, de communicatie tussen de verschillende kabinetten van de Belgische federale overheid verzekert door middel van een postdienst. De feiten zijn de volgende[38] : een oud-medewerker van het kabinet van de toenmalige eerste minister, Leo Tindemans, en een vriend van eerstgenoemde, verschaften zich tussen augustus en oktober

[29] M. MCGUIRE, *Hypercrime: The New Geometry of Harm*, New York, Routledge-Cavendish, 2007, 1-3.
[30] M. YAR, *Cybercrime and society*, Londen, Sage Publications ltd, 2006, 7.
[31] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 21.
[32] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 22.
[33] Convention on cybercrime Council of Europe ETS no. 185, 2001. Budapest.
[34] Rb. Brussel 8 november 1990, *Computerr.* 1991, (31) 31.
[35] http://cwisdb.kuleuven.be/pisa/nl/juridisch/crack.htm.
[36] J. DUMORTIER, *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 122.
[37] B. DE SCHUTTER, "Het Belgische Bistel-syndroom", *Computerr.* 1991, (164) 165.
[38] B. DE SCHUTTER, "Het Belgische Bistel-syndroom", *Computerr.* 1991, (164) 166.

1988 toegang tot het BISTEL-systeem. Zij verkregen toegang tot het netwerk door gebruik te maken van de toegangscode van de eerste minister en een medewerkster van zijn kabinet. Niet alleen verschaften zij zichzelf toegang tot vertrouwelijke informatie toebehorend aan de Belgische staat en de eerste minister, ze maakten tevens het gebruik van het BISTEL-systeem onmogelijk voor de eerste minister en zijn kabinetsmedewerkster. De computerinbraak in kwestie kwam aan het licht, en de twee dienden voor de correctionele rechtbank te verschijnen. De twee beklaagden werden veroordeeld op basis van drie gronden[39] [40]:

- valsheid in geschriften: beiden hadden gebruik gemaakt van een toegangscode die hen geenszins toebehoorde. Gebruikmakend van deze toegangscode hebben zij zich daarenboven voorgedaan als zijnde rechtmatige gebruikers van het BISTEL-systeem. De correctionele rechtbank oordeelde dat in dit kader het paswoord kon worden beschouwd als zijnde een geschrift;
- diefstal van computerenergie: de correctionele rechtbank oordeelde dat het onrechtmatig gebruik van de toegangscode een verzwarende omstandigheid uitmaakte. De rechtbank beschouwde dit onrechtmatig gebruik als een diefstal met braak, inklimming, of het gebruik van valse sleutels;
- verduistering van de aan de RTT (toenmalige Regie voor Telegraaf en Telefoon) toevertrouwde mededelingen om kennis te nemen van de inhoud ervan.

31. Tegen deze uitspraak van de correctionele rechtbank werd echter beroep aangetekend. Voor het hof van beroep werd het grootste deel van bovenstaande uitspraak naar de prullenmand verwezen. Het hof:

- stelde dat een toegangscode geen geschrift is in de zin van artikel 193 Sw.
- oordeelde vervolgens ook dat de beide beklaagden geenszins de bedoeling hadden computerenergie te stelen.
- volgde de redenering van de correctionele rechtbank omtrent verduistering van gegevens aan de RTT. Beide beklaagden werden dan ook vervolgd op grond van de RTT-wet van 1930[41], die vervangen werd door de wet van 1991 op de economische overheidsbedrijven.[42]

[39] Rb. Brussel 8 november 1990, *Computerr.* 1991, (31) 31.
[40] http://cwisdb.kuleuven.be/pisa/nl/juridisch/crack.htm.
[41] Wet 19 juli 1930 tot oprichting van de Regie van Telegraaf en Telefoon, *B.S.* 2 augustus 1930.
[42] Wet 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.* 27 maart 1991.

32. In de nasleep van de BISTEL-zaak werd het duidelijk dat onze Belgische regelgeving onvoldoende aangepast was om op te treden tegen dergelijke inbreuken. De correctionele rechtbank poogde dit euvel enigszins te camoufleren door analoge toepassingen van bestaande incriminaties op computerinbraak te aanvaarden. Het hof van beroep daarentegen kon zich allerminst vinden in deze redenering. Hoe dan ook, het is duidelijk dat de Belgische wetgeving op dat tijdstip niet aangepast was, er moesten nieuwe wetgevende initiatieven genomen worden. Deze initiatieven kwamen er ook in de vorm van de wet inzake informaticacriminaliteit.[43]

2. OMSCHRIJVING VAN HET CONCEPT CYBERCRIME

2.1 Definitie

33. Ondanks het feit dat het woord cybercrime een wijd verspreid begrip is, is het niet zo vanzelfsprekend om de term te definiëren. Dit wordt in de hand gewerkt door het feit dat er geen catch-all bepaling is van wat cybercrime nu juist inhoudt. Cybercrime heeft immers een veelvoud aan facetten en komt op allerhande manieren voor. Het is daarom ook doeltreffender om cybercrime niet te zien als zijnde één crimineel fenomeen, maar als een brede waaier van inbreuken. De bestaande definities van cybercrime zijn in elk geval doorheen de tijd sterk geëvolueerd. Ze verschillen in die zin vooral door de verschillende percepties van waarnemers en slachtoffers, evenals door het verloop van tijd en de daarbij horende technologische vooruitgang.

34. De Raad van Europa heeft in zijn Cybercrime-Verdrag[44] geprobeerd cybercrime te definiëren. De Raad ziet cybercrime als "*alle strafbare gedragingen die gericht zijn tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van geautomatiseerde processen en middelen (computercriminaliteit in enge zin) en de strafbare handelingen die zich richten op het verstoren of beïnvloeden van de werking van computersystemen of met die systemen onderhouden geautomatiseerde processen (computercriminaliteit in brede zin)*". [45] [46] De Verenigde Naties definieerden cybercrime tijdens het 'Tenth United Nations Congress on the

[43] Wet 28 november 2000 inzake informaticacriminaliteit, *B.S.* 3 februari 2001.
[44] Convention on cybercrime Council of Europe ETS no. 185, 2001. Budapest.
[45] http://profs.sci.univr.it/~giaco/download/Watermarking-Obfuscation/cybercrime%20classification.pdf.
[46] M. YAR, *Cybercrime and society*, Londen, Sage Publications ltd, 2006, 9.

Prevention of Crime and the Treatment of Offenders' in april 2000, te Wenen. De definitie luidt als volgt : *"Elk misdrijf dat kan gepleegd worden in een elektronische omgeving en waar men onder een misdrijf het vergrijp verstaat dat in het algemeen als onwettig wordt beschouwd of meestal wel gesanctioneerd wordt."* [47] [48]Rechtsgeleerden houden er eveneens vaak andere definities op na. Zo definiëren Thomas en Loader cybercrime als *"computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through to global electronic networks"*.[49]

35. Het is hoe dan ook duidelijk dat cybercrime een zogenaamd containerbegrip is. Cybercrime is en blijft een verzamelterm voor tal van uiteenlopende gedragingen. De wijze waarop men cybercrime interpreteert hangt nauw vast met de wetenschappelijke discipline die het begrip hanteert. Zo zal cybercrime een andere invulling hebben wanneer de term wordt gebruikt door een verzekeringsexpert, een informaticus of een jurist.[50]

2.2 Factoren die cybercrime in de hand werken

36. Doorgaans wordt er in het algemeen strafrecht van uitgegaan dat er drie factoren zijn die een voedingsbodem vormen voor crimineel gedrag. Vooreerst dienen er mensen te zijn die überhaupt overwegen het misdrijf te plegen. Vervolgens moet zich de opportuniteit voordoen om effectief over te gaan tot het plegen van het misdrijf. Tenslotte dient er een afwezigheid te zijn van een instantie die het plegen van het misdrijf wil tegengaan. De digitale wereld vormt een uitstekende voedingsbodem voor alle drie deze punten. Naast deze algemene aspecten zijn er tal van punten die crimineel gedrag in de digitale wereld wezenlijk vergemakkelijken:[51]

- Het uitgestrekt karakter van het internet

  Een van de kenmerken van het internet is haar grootte. Gebruikers kunnen met oneindig veel mensen communiceren, en dat op een goedkope en makkelijke manier. Men gaat er van uit dat er wereldwijd ongeveer 1.6 miljard mensen van het internet gebruik maken. Dit geeft misdadigers de mogelijkheid om op een erg grote schaal te opereren.[52]

[47] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 381.
[48] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 23.
[49] M. YAR, *Cybercrime and society*, Londen, Sage Publications ltd, 2006, 9.
[50] http://pubs.cli.vu/pub168.php.
[51] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 5.
[52] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 5.

- De toegankelijkheid van het internet

  Begin de jaren ’80 waren computers voorwerpen die praktisch uitsluitend werden gebruikt door overheden. Computercriminaliteit was op dat punt dan ook nog geen probleem. Meer recent is het gebruik van een computer ook bij de gewone bevolking ingebed. De technologie op zich is makkelijk te gebruiken en leent zich dus ook in zekere zin tot misbruiken.[53]

- De anonimiteit van het internet

  Het internet biedt zijn gebruikers een zekere vorm van anonimiteit. Dit kan een enorm voordeel bieden voor misdadigers. De kans op betrapping is in de virtuele wereld dan ook vele malen lager dan bij misdrijven in het echte leven.[54]

- De afwezigheid van landsgrenzen

  Strafrecht is steeds beperkt tot een bepaald grondgebied, waar het misdrijf zich heeft voorgedaan. Het internet volgt deze regels echter niet, het is een globaal medium. Voor misdadigers betekent dit een wereld van opportuniteiten. Voor het recht daarentegen, is het een nachtmerrie.[55]

- Afwezigheid van controlerende instanties

  Volgens de theorie van de rationele misdadiger maakt een crimineel steeds een kosten-batenanalyse, waarbij hij nagaat wat het voordeligst is, het misdrijf al dan niet plegen. In dit opzicht is de afwezigheid van een toezichthoudende instantie met betrekking tot het internet een groot nadeel. Criminelen krijgen aldus de perceptie dat ze ongrijpbaar zijn, ongeacht het misdrijf dat ze plegen. In zekere zin is dat effectief ook zo, het groot aantal gebruikers en het vluchtige karakter van een medium als internet maakt het voor politiële instanties bijzonder moeilijk om adequaat in te grijpen.[56]

2.3 Constitutieve bestanddelen van cybercrime

37. Om de constitutieve bestanddelen[57] van cybercrime te bepalen, kunnen we in eerste instantie teruggrijpen naar het algemene strafrecht. Traditioneel wordt een misdrijf in twee elementen opgedeeld, een materieel en een moreel element. Dit onderscheid tussen actus reus

[53] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 5.
[54] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 6.
[55] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 7.
[56] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 8.
[57] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen*, II, Antwerpen, Maklu, 2009, 186-189.

en mens rea kadert in het klassieke 19de eeuwse mensbeeld, waar de dualiteit tussen geest en lichaam centraal stond. Het materiële element van een misdrijf heeft betrekking op de uiterlijke verschijningsvorm van het misdrijf. Het betreft de gedraging an sich, die een inbreuk op de strafwet uitmaakt. Het moreel element, daarentegen, heeft betrekking op de schuldvorm waarmee de gedraging in kwestie wordt gesteld. Het betreft hier het opzet, de onachtzaamheid, en in zekere zin ook de afwezigheid van één of meerdere schulduitsluitingsgronden. Naast deze twee klassieke elementen worden in de rechtsleer vaak nog andere constitutieve bestanddelen onderscheiden. Zo is een vaak voorkomend derde constitutief element de wederrechtelijkheid. Dit laatste heeft betrekking op de afwezigheid van rechtvaardigingsgronden. Meer bepaald wordt er gedoeld op het feit dat het misdrijf niet voltrokken is door de loutere aanwezigheid van het in de wet bepaalde materieel en moreel element, er is tevens dat de handeling in kwestie niet gerechtvaardigd is. Ook het element strafwaardigheid wordt bijwijlen aanzien als een constitutief bestanddeel, net als een wettelijk element.

38. In dit onderdeel zal er dieper worden ingegaan op het materiële element, de uiterlijke verschijningsvormen van cybercrime. Zoals reeds besproken werd bij de definitie van cybercrime, blijkt opnieuw dat het allesbehalve een sinecure is om te bepalen wat nu wel en niet onder de term cybercrime wordt verstaan. Gezien het formuleren van een sluitende definitie, voor deze vorm van criminaliteit, heel wat voeten in de aarde had [58] [59], opteerde men na verloop van tijd voor een classificatie van de verschillende gedragingen, eerder dan voor een enge definitie van het probleem. Er werd een onderscheid gemaakt tussen specifieke- en a-specifieke informaticacriminaliteit. Datzelfde onderscheid vinden we zowel terug in het Cybercrime-Verdrag van de Raad van Europa [60], als in onze wet inzake informatica-criminaliteit.[61]

[58] P. VAN EECKE, *Criminaliteit in Cyberspace: Misdrijven, hun opsporing en vervolging op de informatiesnelweg*, Gent, Mys en Breesch, 1997, 15.
[59] B. SPRUYT, "Computers op de strafbank" in B. DE SCHUTTER, *Informaticacriminaliteit*, Kluwer, Antwerpen-Deventer, 1987, (232) 234.
[60] Convention on cybercrime Council of Europe ETS no. 185, 2001. Budapest.
[61] Wet 28 november 2000 inzake informaticacriminaliteit, *B.S.* 3 februari 2001.

2.3.1 Specifieke informaticacriminaliteit

2.3.1.1 Begrip

39. Specifieke informaticacriminaliteit omvat die gedragingen waarbij het gebruik van telematica een noodzakelijke rol speelt. Het informaticasysteem vormt hier met andere woorden een constitutief bestanddeel van het misdrijf. Zonder het gebruik van het informaticasysteem zou er geen sprake zijn van het misdrijf. Er werd in dit kader geopteerd voor een classificatie van de verschillende gedragingen die onder deze categorie dienen te worden verstaan. Dit geschiedde onder invloed van de OESO[62] en de Raad van Europa. De betrokken classificatie gaat uit van de verschillende vormen van informaticamisbruik die op dat moment bekend waren. De Raad van Europa stelde in dit kader volgende minimumlijst met laakbare gedragingen op: [63] [64] [65]

- *Computer related fraud:*

  the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person made with the intent of procuring an unlawful economic gain for oneself or for another person or with the intent to unlawfully deprive that person of his property;
- *Computer forgery:*

  the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would substitute the offence of forgery if it had been committed with respect to traditional object of such an offence;
- *Damage to computer data and computer programs:*

  the erasure, damaging, deterioration or suppression of computer data or computer programs without right;

[62] OESO staat voor Organisatie voor Economische Samenwerking en Ontwikkeling.
[63] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 15-16.
[64] Recommendation Council of Europe No. R (89) 9 adopted by the Committee of Ministers of the Council of Europe, 13 september 1989, concerning Computer-Related Crime.
[65] Report of the European Committee on Crime Problems, 1990, Strasbourg.

- *Computer sabotage:*

  the input, alteration, erasure or suppression of computer data or computer programmes, or other interference with the course of data processing, with the intent to hinder the functioning of a computer or a telecommunication system;
- *Unauthorized access:*

  the access without right to a computer system or network by infringing security measures;
- *Unauthorized interception:*

  the interception, made without right end by technical means, of communication to, from and within a computer system or network;
- *Unauthorized reproduction of a protected computer program:*

  the reproduction, distribution or communication to the public without right of a computer program which is protected by law;
- *Unauthorized reproduction of topography:*

  the reproduction without right of topography, protected by law, of a semiconductor product, or the commercial exploitation or the importation for that purpose, done without the right of a topography or a semiconductor product manufactured by using the topography.

2.3.1.2 Computerinbraak

40. Computerinbraak of hacking, is een fenomeen dat zich voordoet wanneer iemand op één of andere manier op ongeoorloofde wijze binnendringt in een computersysteem. Het betreft met andere woorden de situatie waarin een gebruiker zich opzettelijk toegang verschaft tot een netwerk, een server of een bestand waarvoor hij geen toestemming heeft, of onopzettelijk deze verbinding tot stand brengt, maar dan toch besluit deze te handhaven.[66] [67] Dit fenomeen is eigen aan het internetgebeuren an sich[68], sinds de introductie van computers en de opkomst van internetverbindingen is er sprake van computerinbraak. Een meer recentere ontwikkeling is dat het hacken of kraken van computers niet langer is voorbehouden voor het kruim onder de computerprogrammeurs, maar in handbereik ligt van eenieder die toegang heeft tot het internet. Dit dankzij tal van 'gebruikshandleidingen' die op het internet circuleren. Wellicht

[66] O. HANCE, *Business op Internet volgens de wet*, Brussel, Mcgraw-hill education, 1996, 210.
[67] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 18.
[68] W.P. STOL, R.J. VAN TREECK en A.E.B.M. VAN DER VEN, "Criminaliteit met ICT", *Modus* 2000, 8-13.

het meest specifieke kenmerk van computerinbraak is zijn heimelijk karakter. De eigenaar van de computer in kwestie heeft in het gros van de gevallen geen flauw benul van wat hem overkomt. Hackers hanteren namelijk softwareprogramma's die zich onopgemerkt op een computer nestelen, na het openen van een bepaalde mail of het bezoeken van een website. Eens dit programma toegang heeft gekregen tot een computer zal de inhoud van de harde schijf toegankelijk worden voor eenieder die er interesse in heeft.

41. Recent zagen we welke verregaande gevolgen dergelijke computerinbraken kunnen hebben. Wanneer eind 2010 de website Wikileaks onder druk kwam te staan om te stoppen met de publicatie van geheime diplomatieke post van de Verenigde Staten, leerde het grote publiek de hackersgroep 'Anonymous' kennen.[69] Zij betuigde kort na deze waarschuwingen haar steun aan Wikileaks en lanceerde aanvallen op PayPal, Mastercard, VISA en de bank PostFinance. Door deze aanval werden de websites van de respectievelijke bedrijven enige tijd compleet lam gelegd. Dat zulke inbraakpogingen schering en inslag zijn, wordt hoe langer hoe meer duidelijk. Experten spreken over meer dan 72.000 inbraakpogingen per dag wereldwijd.[70] [71]

2.3.1.3 Manipulatie van elektronische gegevens

42. De manipulatie van elektronische gegevens kan omschreven worden als het toevoegen, het wijzigen, het verwijderen of het overnemen van deze gegevens. Met elektronische gegevens worden zowel data als programma's bedoeld. Typische vormen van manipulatie van data zijn het vervalsen van invoergegevens of computerbestanden.[72] Ook het laten infiltreren van computervirussen of zogenaamde Trojaanse paarden wordt onder deze noemer gecatalogeerd. De Belgische wetgeving voorziet een aantal mogelijkheden om de manipulatie van elektronische gegevens te bestraffen. Men dient een onderscheid te maken tussen twee situaties. Enerzijds, kan men de bestraffing eisen van een materiële handeling, met name het ongeoorloofd manipuleren van computergegevens. Anderzijds, kan men de beoogde doelstelling bestraffen, namelijk het zich verschaffen van een vermogensvoordeel, het beschadigen van andermans belangen of het beïnvloeden van diens beslissingen. Wanneer

[69] D. DECKMYN, "Het cyberleger van Assange", *De Standaard* 12 december 2010, www.destandaard.be.
[70] R.L. DUNNE, "Deterring unauthorized access to computers: controlling behavior in cyberspace through a contract paradigm*", Jurimetrics* 1994, 1-15.
[71] O. HANCE, *Business op Internet volgens de wet*, Brussel, Mcgraw-hill education, 1996, 210.
[72] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 27-29.

men kiest voor de eerste optie dient men zich te beroepen op de figuur van de valsheid in geschrifte. Optie twee biedt een ruimer pallet aan incriminaties, met name diefstal, oplichting, valsmunterij alsmede misbruik van vertrouwen.

2.3.1.4 Illegaal kopiëren of verspreiden van computersoftware

43. Dit betreft het kopiëren en verspreiden van computerprogramma's met het doel het betalen van auteursrechten te ontwijken.

2.3.1.5 Illegaal kopiëren van software

44. Het opzet betreft het namaken van het origineel product, om het vervolgens als zijnde origineel te verkopen. [73]De consument vertrouwt, ten onrechte, op het feit dat hij een origineel softwarepakket heeft aangeschaft.

2.3.1.6 Illegaal kopiëren van muziek

45. Dit is wellicht de meest bekende en meest toegepaste vorm van informaticacriminaliteit. LimeWire, Napster en The Pirate Bay zijn maar enkele van de vele websites die voorzien in de mogelijkheid om gratis te downloaden. Zij zijn verantwoordelijk voor de teloorgang van de klassieke cd-verkoop en zijn al jaren een doorn in het oog van de muziekindustrie.

2.3.1.7 Informaticabedrog

46. Informaticabedrog heeft betrekking op het manipuleren van elektronische gegevens om een zeker vermogensvoordeel te bekomen. Dit alles geschiedt door het inbrengen van fictieve namen in een bestand of het aanpassen van bepaalde gegevens.

2.3.1.8 Valsheid in informatica

47. Deze categorie is ingevoerd door de Belgische wet inzake informaticacriminaliteit van 28 november 2000. Een goed voorbeeld binnen deze categorie is het vervalsen van kredietkaarten.[74]

[73] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 50.
[74] E.J. DUMORTIER, "Het auteursrecht spoelt weg door het elektronische vergiet. Enige gedachten over de naderende crisis van het auteursrecht", *Computerr.* 1994, (109) 109-110.

2.3.2 A-Specifieke informaticacriminaliteit

2.3.2.1 Begrip

48. Er is sprake van a-specifieke informaticacriminaliteit wanneer de informatica of telecommunicatie louter een middel is om een misdrijf te plegen. Het misdrijf is in dit geval niet omwille van zijn aard verbonden aan een informaticasysteem. [75]Het informaticasysteem heeft hier de loutere rol van middel, een modus operandi, om het misdrijf te plegen. In alle onderstaande gevallen wordt het informaticasysteem gebruikt als medium om een misdrijf te plegen, maar maakt het systeem zelf geen constitutief bestanddeel uit van het misdrijf.

2.3.2.2 Illegale verspreiding van pornografie

49. Pornografisch materiaal is in ruime mate verkrijgbaar op het internet. Uit een Amerikaanse studie[76] blijkt dat een belangrijk deel van de pornografische informatie die op netwerken verspreid worden, bestaat uit beelden en teksten met de nadruk op pedofilie en andere vormen van seksueel afwijkend gedrag. Dat dit zo ruim verspreid is, hoeft niet te verbazen, omwille van verschillende redenen. De technologie is eindeloos, nieuw materiaal kan met de regelmaat van de klok openbaar worden gemaakt. Ook de grote toegankelijkheid van het internet werkt dit in de hand. Maar de voornaamste reden is de schijn van ongrijpbaarheid, het gevoel van anonimiteit die het internet zijn gebruikers biedt. Dergelijk materiaal bereikt op allerlei wijzen zijn bestemming. E-mail, nieuwsgroepen, internet relay chat, het World Wide Web zelf, alsook een Bulletin Board-systeem, bieden elk de mogelijkheid tot een snelle verspreiding. Dit alles kwam recent nog in de media. Het programma 'Undercover in Nederland' van de Nederlandse zender SBS 6 legde in een reportage bloot hoe een Belgische man probeerde om via tussenpersonen in contact te komen met minderjarige meisjes, met de bedoeling hen te misbruiken.[77] De man in kwestie gebruikte het Tor-netwerk, dat volledig anoniem surfen mogelijk maakt.

[75] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 16.
[76] M. RIMM, "Marketing Pornography on the information Superhighway", *Georgetown Law Journal* 1995, 1849-1934.
[77] C. LAGAST, "Vlaamse kinderverkrachter opgepakt na Nederlandse undercover-reportage", *De Standaard* 12 februari 2012, www.destandaard.be.

2.3.2.3 Bestraffing van de aanranding van de eer of de goede naam van personen

50. Aanranding van de eer of de goede naam krijgt door het opkomen van moderne technologie een veel bredere context dan voorheen.[78] Het internet bereikt een onmetelijk grote gemeenschap. De schade aan de eer en de goede naam, met behulp van dit medium, is onnoemelijk groot. Zo was er in 2011 een rechtszaak voor de arbeidsrechtbank van Leuven. Een werknemer had op zijn facebookprofiel zijn ongezouten mening gegeven over zijn werkgever. De werknemer in kwestie had een openbaar profiel, met als gevolg dat de hele wereld zijn bevindingen kon lezen. De werknemer maakte zich op deze manier onmogelijk binnen het bedrijf, wat leidde tot zijn ontslag om dringende reden. De werknemer stapte naar de rechtbank, waar hij in het ongelijk werd gesteld.[79]

2.3.2.4 Bestraffing van racistische uitlatingen en ontkenning van de genocide

51. Cyberspace biedt ook opportuniteiten voor extremisten om extremistische of revisionistische boodschappen te verspreiden.[80] Zo gebruikt Sharia4Belgium een forum op internet om haar extremistische boodschappen de wereld in te sturen.

2.3.2.5 Aanzetten tot crimineel gedrag

52. Via internet kan eenieder informatie verkrijgen over onderwerpen die in onze maatschappij niet kunnen worden getolereerd. Zo zijn er op internet tal van doe-het-zelf cursussen te vinden die betrekking hebben op het vervaardigen van springtuigen[81], het uitvoeren van aanslagen e.d.. Deze informatie is ook in de echte wereld te verkrijgen. Het probleem stelt zich echter op die manier, dat de info in de virtuele wereld slechts enkele muisklikken verwijderd is.

2.3.2.6 Gokken

53. Waar in België het uitbaten van een gokgelegenheid streng is gereglementeerd, is de toegang tot gok sites op internet veel eenvoudiger. Dit heeft niet alleen nefaste gevolgen met het oog op een gokverslaving an sich. Deze sites worden eveneens gebruikt voor andere

[78] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 64-65.
[79] B. VAN DEN BROUCKE, "Kritiek over werkgever op Facebook reden tot ontslag", *Het Nieuwsblad* 17 november 2011, www.nieuwsblad.be.
[80] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 66.
[81] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 68.

malafide praktijken, zoals het witwassen van opbrengsten uit andere illegale activiteiten.[82] Vele internetcasino's voorzien namelijk de mogelijkheid om een offshore account aan te maken. Het is duidelijk dat het internet op deze manier bijdraagt dat er een internationaal gokcircuit ontstaat dat grotendeels ontsnapt aan overheidscontrole.

2.3.2.7 Oplichting

54. Cyberspace is een gedroomde speeltuin voor elke oplichter, de mogelijkheden om zichzelf op onrechtmatige wijze te verrijken via het internet zijn eindeloos.[83] Er zijn tal van voorbeelden in dit kader. Zo zijn er gevallen bekend waarin men een mail krijgt met de melding dat men het winnend lot heeft gewonnen bij één of andere buitenlandse loterij. Om de prijs te claimen dient men eerst via Western Union een bedrag op een rekening over te maken. Soortgelijk is het verhaal dat men erfgenaam is van een rijk familielid in het buitenland. Het bedrag van de erfenis kan maar bekomen worden als men zelf eerst geld overmaakt. Een ander bekend voorbeeld situeert zich in de telecomsector. Men kan een betaallijn aanvragen bij bijvoorbeeld Belgacom, waarbij elke oproeper een bepaald bedrag bovenop de verbindingskosten betaalt. Dit bijkomend bedrag wordt tussen Belgacom en de uitbater van de lijn betaald. De uitbater zelf belt echter voortdurend naar zijn eigen nummer, door middel van vaste calling cards of via een valse GSM. De uitbater zal door Belgacom dan procentueel vergoed worden voor de gemaakte telefoonverbindingen. De telefoonrekeningen van Belgacom aan de oproeper zullen echter nooit worden betaald.[84] Eveneens populair zijn het aanbieden van niet-bestaande diensten of goederen. Zo worden er met de regelmaat van de klok pogingen ondernomen om valse aandelen, onbestaande vastgoedprojecten, valse abonnementen e.d. te slijten.

2.3.3 Recente categorisering

55. De meest recente, en veelgebruikte, categorisering van cybercrime vinden we terug in het Cybercrime-Verdrag van de Raad van Europa.[85] Het verdrag in kwestie maakt een grote opsplitsing tussen cybercrime sensu lato en cybercrime sensu stricto. Cybercrime sensu stricto

[82] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 74.
[83] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 77.
[84] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 78-79.
[85] Convention on cybercrime Council of Europe ETS no. 185, 2001. Budapest.

geldt in het Cybercrime-Verdrag als verzamelnaam voor zogenaamde C.I.A.-delicten.[86] Laatstgenoemden zijn delicten die inbreuken vormen tegen de begrippen Confidentiality, Integrity en Availalibility.[87] Deze delicten zijn erop gericht bepaalde maatschappelijk aanvaarde waarden en normen te doorbreken. Meer specifiek viseert de Raad van Europa volgende feiten:

- het zich wederrechtelijk onbevoegd toegang verschaffen tot een computersysteem;
- het wederrechtelijk onderscheppen van gegevensverkeer;
- het wederrechtelijk wijzigen, wissen of ontoegankelijk maken van gegevens die door een computersysteem worden verwerkt;
- het wederrechtelijk verstoren van de goede werking van een computersysteem.

56. Deze categorie viseert ook pogingen tot bovenstaande delicten, evenals medeplichtigheid eraan. Ook het vervaardigen en ter beschikking stellen van instrumenten, programma's of codes die deze inbreuken mogelijk maken vallen onder de bepaling.

57. Cybercrime sensu lato is gebaseerd op drie pijlers en maakt een onderscheid tussen volgende delicten:

- vooreerst wordt computergerelateerde criminaliteit geviseerd. Het betreft hier vooral fraude en valsheid in geschriften met betrekking tot ICT. Deze categorie omvat bijvoorbeeld fraude met elektronische betaalmiddelen en oplichting op het internet in het algemeen;[88]
- vervolgens zijn er de inbreuken op het gebied van auteursrecht en aanverwante rechten met betrekking tot ICT;[89]
- tenslotte worden inhoudgerelateerde delicten geviseerd. Het verdrag viseert met name uitings- en verspreidingsdelicten. In dit kader worden onder meer de productie en verspreiding van kinderporno geviseerd, evenals het aanbieden van illegale kansspelen of producten waarvan het aanbod als dusdanig onderhevig is aan nationale beperkingen.[90]

[86] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 9-10.
[87] H.W.K. KASPERSEN, *Schriftelijke leergang Nieuwe Telecomwet*, Hilversum, Broadcast Press, 2004, http://pubs.cli.vu/pub168.php.
[88] H.W.K. KASPERSEN, *Schriftelijke leergang Nieuwe Telecomwet*, Hilversum, Broadcast Press, 2004, http://pubs.cli.vu/pub168.php.
[89] H.W.K. KASPERSEN, *Schriftelijke leergang Nieuwe Telecomwet*, Hilversum, Broadcast Press, 2004, http://pubs.cli.vu/pub168.php.
[90] H.W.K. KASPERSEN, *Schriftelijke leergang Nieuwe Telecomwet*, Hilversum, Broadcast Press, 2004, http://pubs.cli.vu/pub168.php.

2.4 De nefaste gevolgen van cybercrime

58. Dat cybercrime een ongewenst neveneffect is van een medium als internet, is duidelijk. De vraag blijft echter welke impact cybercrime heeft op particulieren, bedrijven, als de economie in zijn geheel. Het antwoord op die vraag is eenduidig, cybercrime heeft een erg grote impact.

59. Norton by Symantec[91] publiceert jaarlijks een cybercrime rapport.[92] Uit de meest recente editie, die van 2011, blijkt dat de schade die cybercrime aanricht enorm is. Het rapport geeft een weergave van de schade die cybercrime wereldwijd aanricht, gevolgd door cijfers per land of regio. Wereldwijd bedroegen de directe kosten vorig jaar maar liefst 114 miljard dollar.[93] Daarnaast leden slachtoffers 227 miljard dollar schade, enkel en alleen al door de tijd die ze verloren zagen gaan door cybercrime.[94] Geschat wordt dat de markt voor marihuana, cocaïne en heroïne goed zou zijn voor een opbrengst van 205 miljard euro. De omvang van de wereldwijde handel in drugs zou goed zijn voor 292 miljard euro, een bedrag dat niet zoveel hoger ligt dan de opbrengsten uit cybercrime.[95] [96]

60. De cijfers voor ons land zijn al even onthutsend. Volgens Symantec zouden vorig jaar zowat 1,4 miljoen Belgen het slachtoffer geworden zijn van cybercriminaliteit.[97] Dit komt neer op gemiddeld drie gedupeerde Belgen per minuut. Samen leden zij ruim 347 miljoen euro verlies. Het rechtstreekse verlies in dit kader bedroeg 160 miljoen euro, de indirecte schade wordt geraamd op 187,5 miljoen euro. Uit de cijfers blijkt tevens dat de helft van de Belgen die online actief zijn al eens het slachtoffer zijn geworden van internetcriminelen. Gelijklopend met de evolutie van het internet blijkt dat maar liefst 56% van die groep voor het

[91] Symantec is een Amerikaans bedrijf dat zich bezig houdt met informatiebeveiliging. Het voorziet in oplossingen die de beveiliging, beschikbaarheid en integriteit van informatie waarborgen voor bedrijven en particulieren. Het hoofdkantoor is gevestigd in Mountain View in de Verenigde Staten.
[92] http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport.
[93] M. VAN DER VEN, "Cybercriminaliteit maakt 3 Belgische slachtoffers per minuut", *De Tijd* 26 september 2011, www.tijd.be.
[94] M. VAN DER VEN, "Cybercriminaliteit maakt 3 Belgische slachtoffers per minuut", *De Tijd* 26 september 2011, www.tijd.be.
[95] www.security.nl/artikel/38404/1/Symantec%3A_Cybercrime_evenaart_drugshandel.html.
[96] De vergelijking tussen de opbrengsten van cybercrime en drugshandel werden gemaakt door David DeWalt, niet toevallig de CEO van McAfee.
[97] M. VAN DER VEN, "Cybercriminaliteit maakt 3 Belgische slachtoffers per minuut", *De Tijd* 26 september 2011, www.tijd.be.

eerst slachtoffer werd in 2010.[98] De grootte van dit aantal ligt hem deels in een verkeerde perceptie aangaande cybercrime, aldus Symantec. Mensen realiseren zich te weinig dat ze wel degelijk een risico lopen op het internet. Dat dit risico zeer reëel is, wordt eens te meer bevestigd door het gegeven dat het aantal slachtoffers van cybercrime liefst drie keer hoger ligt dan het aantal dat met fysieke criminaliteit te maken krijgt. Gebruikers dienen zich dan ook beter te wapenen tegen deze relatief nieuwe vorm van criminaliteit. Dit kan door zeer eenvoudig de beveiligingssoftware up-to-date te houden, of voor complexe wachtwoorden te opteren.

61. De meest voorkomende vormen van cybercrime blijven computervirussen en malware, en in mindere mate phishing mails en hacking. Het aantal slachtoffers die te maken krijgt met cybercriminaliteit via een mobiele telefoon ligt dan weer opvallend lager dan de wereldwijde tendens.[99]

62. Het Computer Emergency Response Team, of kortweg CERT genaamd, komt met ietwat lagere cijfers voor de dag. Het CERT is een publieke dienst met als doel de Belgische bevolking te voorzien van informatie omtrent computerbeveiliging.[100] Per maand lopen er bij het CERT 100 tot 200 incidenten binnen omtrent cybercrime, al stelt Jan Torreele, technisch directeur van BELNET,[101] dat er in realiteit een veelvoud aan incidenten plaatsvinden.[102] Toch zijn er ook stemmen te horen die stellen dat Symantec en McAfee bovenstaande cijfers enigszins overdrijven, en dat de vergelijking met de wereldwijde opbrengst van drugshandel kant noch wal raakt. Richard Stiennon, een security analist bij IT-Harvest, is één van die stemmen. Volgens laatstgenoemde is cybercrime uberhaupt niet te vergelijken met drugshandel, niet wat betreft de betrokken mensen, de slachtoffers, de impact en dergelijke meer. Niettemin onderkent hij de ernst van cybercrime, en is hij eveneens de mening toegedaan dan we, als maatschappij, niet in het minst zijn voorbereid op de escalatie van cybercrimegevallen.[103]

[98] M. VAN DER VEN, "Cybercriminaliteit maakt 3 Belgische slachtoffers per minuut", *De Tijd* 26 september 2011, www.tijd.be.
[99] http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport.
[100] www.cert.be/citizen/nl.
[101] Belnet is het Belgian National Research and Education Network.
[102] K. CLERIX, "Gemiddeld 100 tot 200 cybercrime-incidenten per maand in België", *MO* 17 november 2010, www.mo.be.
[103] R. STIENNON, "Cyber crime is not bigger than illegal drug trade", *ZDNet* 19 september 2007, www.zdnet.com.

63. In elke situatie is het aangewezen na te gaan van wie bepaalde informatie afkomstig is. Wanneer we het bovenstaande op een kritische wijze bekijken, dienen we er ons bewust van te zijn dat Symantec en McAfee, twee grootmachten inzake beveiligingssoftware, hun cijfers zeker niet zullen minimaliseren. Het zijn bedrijven gericht op het maken van zoveel mogelijk winst. Het grote publiek angst inboezemen voor een fenomeen als cybercrime, zal in dat opzicht dan ook niet nefast zijn voor hun respectievelijke bedrijfsresultaten. Niettemin dienen we de ernst van de situatie wel degelijk te erkennen. Cybercrime maakt, wat nu ook de exacte cijfers zijn, veel slachtoffers en heeft zonder twijfel ook een grote financiële impact op onze maatschappij.

3. EEN RECENTE VORM VAN CYBERCRIME: HET TOR-NETWERK

3.1 Inleiding

64. Dat het internet zich leent tot crimineel gedrag behoeft geen betoog, het grote aantal typische en a-typische informaticamisdrijven spreekt in dit kader boekdelen. Wat criminelen in dit opzicht enigszins kan tegenhouden is de traceerbaarheid die het World Wide Web met zich meebrengt. Niettemin het merendeel van de bevolking de mening toegedaan is dat surfen op het internet volledig anoniem kan verlopen, is dit slechts een illusie. Elke internetgebruiker is immers opspoorbaar via het IP-adres. In die zin biedt dit IP-adres een wapen om de ongebreideldheid van het internet tegen te gaan. Recent bleek echter dat dit alles kinderlijk eenvoudig kon worden omzeild via zogenaamde parallelcircuits. Het zogenaamde ‘Darknet’, en het hieraan verbonden programma Tor, maakt het immers mogelijk om volkomen anoniem te surfen. Het klassieke internet bestaat uit computers waarvan het adres is opgenomen in de Domain Name Server (DNS), een soort centrale adressenbestand van het internet. Vroeger was er heel wat informaticakennis vereist om op verborgen servers terecht te komen. Nu volstaat het echter om één stuk software te downloaden, de Tor-browser. Dit is een zoveelste terugslag in de strijd tegen informaticacriminalteit

3.2 Wat is Tor?

65. De tijd dat criminelen te werk gingen via het reguliere internet ligt achter ons. Het nieuwe godenkind noemt Darknet, het verborgen internet. Wie echter op Darknet wil moet eerst een

programma installeren, Tor genaamd. Tor is, eenvoudigweg, via google te downloaden. Het programma biedt twee grote voordelen voor criminelen. Het zorgt er, enerzijds, voor dat je volledig anoniem kan surfen. Anderzijds, geeft het toegang tot verborgen servers. Zodra het programma is geïnstalleerd verloopt je eigen internetverkeer niet meer via de gewone weg, maar langs tientallen andere computers. Op deze manier kan je provider, Telenet of Belgacom, niet meer achterhalen welke sites je bezoekt.[104]

66. De startpagina noemt 'The hidden wiki', een soort navigeerkaart doorheen het Darknet. Op deze manier kan je tal van verborgen sites bezoeken. Het assortiment is eindeloos, er is keuze tussen honderden sites. Eén van de populairste is The Silk Road, een online winkel waar drugs en wapens openlijk worden verhandeld. The Silk Road is de meest beruchte webwinkel van het Darknet. De site werkt en ziet eruit als een doorsnee webwinkel. Net als bij Ebay of Amazon heb je een winkelkarretje en makkelijke digitale betalingsmogelijkheden. De producten zijn net als op voorgenoemde sites duidelijk afgebeeld, aangevuld met een beschrijving en de prijs.[105]

67. Op Darknet zijn alle deelgebieden van het criminele spectrum te vinden. Men kan er forums vinden voor extremisten, evenals websites die zich specialiseren in het namaken van rijbewijzen en valse paspoorten. Werkelijk alle diensten worden op het Darknet aangeboden. Ook pedofielen vinden er hun gading. Dit bleek onlangs nog uit een reportage van het programma Undercover in Nederland van de Nederlandse zender SBS 6. Journalist Alberto Steegman ging undercover op het netwerk en ontmaskerde zo een Belgische pedofiel. De producten en diensten worden betaald met Bitcoin, en dat volledig anoniem, gezien ze via Tor verlopen. Bitcoin is een virtuele munt, het betaalmiddel bij uitstek in deze digitale onderwereld. Het is een munteenheid zonder centrale bank of toezichthouder. Computers creëren Bitcoin via wiskundige algoritmen. De betaling geschiedt via kredietkaarten, overschrijvingen of internetdiensten. Bitcoin kreeg vorige zomer plots aandacht van beleggers, omdat de munt in mei een enorme piek kende. Eén bitcoin was op dat moment net geen 20 Euro waard.[106]

[104] D. DECKMYN,"Speeltuin van wapenhandelaars en drugsdealers", *De Standaard* 4 maart 2012, (16) 16.
[105] D. DECKMYN, "Speeltuin van wapenhandelaars en drugsdealers", *De Standaard* 4 maart 2012, (16) 16.
[106] D. DECKMYN, "Speeltuin van wapenhandelaars en drugsdealers", *De Standaard* 4 maart 2012, (16) 19.

68. Misschien wel het meest frappante aan deze zaak is dat Tor geen project is van hackers, integendeel. De technologie werd initieel zelfs ontwikkeld voor de Amerikaanse Navy. De belangrijkste financierder is de Amerikaanse overheid, en ook de Zweedse overheid ondersteunde het project, net als internetgigant Google.[107] Laatstgenoemden stellen dat Tor is ontwikkeld om politieke dissidenten te helpen om te spreken zonder risico op vervolging. Criminelen hebben Tor niet nodig, zo houden zij staande. Volgens hen bestaan er voor criminelen tal van andere manieren om je identiteit te verbergen op het internet.

69. Ook Andrew Lewman, directeur van het Tor-Project, minimaliseert het probleem. Het opzet van Tor is, aldus Lewman, in eerste instantie om groeiende overheidscensuur tegen te gaan. Lewman is zich bewust van het feit dat Tor een gedroomd speeltje is van misdadigers. Hij is echter wel de mening toegedaan dat de nadelen van Tor niet opwegen tegen de voordelen, namelijk de vrije meningsuiting.[108]

3.3 Optreden tegen Tor?

70. Een vraag die zich in dit kader opwerpt is of de politie kan optreden tegen een dergelijk geraffineerd netwerk. Volgens Luc Beirens, hoofd van de Federal Computer Crime Unit (FCCU) ligt dit niet voor de hand.[109] Het probleem zit hem voornamelijk in het feit dat Tor allerhande data codeert, waardoor het voor politionele instanties moeilijk is om de inhoud van een bezochte site na te gaan. Hoewel het gegeven Tor zich situeert in een zweem van misdadigheid, is het louter surfen op het internet met Tor niet strafbaar. We dienen hier wel een onderscheid te maken met het 'volledig anoniem' surfen. Netwerkproviders (zoals Telenet of Belgacom) moeten te allen tijde hun surfers kunnen identificeren. De wet stipuleert in dat opzicht namelijk dat het gebruik van het internet identificeerbaar dient te zijn. Op dit punt bevindt Tor zich dan ook in een juridisch vacuüm, gezien het een volkomen wirwar maakt waardoor de traceerbaarheid nihil is en de wetgeving er bijgevolg geen vat op heeft. Luc Beirens wijst er ook op dat politieagenten zich niet zomaar mogen voordoen als koper of verkoper, om iemand in de val te lokken. Dergelijke infiltratie valt onder de wet op de bijzondere opsporingsmethoden (BOM), waarvan de toepassing aan strikte regels is onderworpen. Volgens Luc Beirens is de strijd tegen Tor dan ook een gevecht tegen de

[107] D. DECKMYN, "De meerderheid wil gewoon kunnen facebooken", *De Standaard* 5 maart 2012,(6) 6.
[108] D. DECKMYN, "De meerderheid wil gewoon kunnen facebooken", *De Standaard* 5 maart 2012,(6) 6.
[109] D. DECKMYN, "Speeltuin van wapenhandelaars en drugsdealers", *De Standaard* 4 maart 2012,(16) 18.

bierkaai.[110] Criminelen maken met kinderlijk gemak gebruik van Tor, in een volledig anonieme, nieuwe wereld. De politie kan als het ware pas optreden als de virtuele criminaliteit zich vertaalt naar welke criminaliteitsvorm dan ook in de reële wereld. Er kan pas opgetreden worden als er effectief drugs wordt gevonden, of als er financiële transacties zichtbaar worden. Wil de FCCU de mogelijkheid hebben om in dit kader op een effectieve wijze op te treden, moeten er twee zaken veranderen, aldus Luc Beirens. Enerzijds, kan men Tor zelf aanpakken, door het gebruik ervan strafbaar te stellen. Anderzijds, kan men tevens opteren voor een uitbreiding van de BOM-wet. Hoe dan ook, er dient werk gemaakt te worden van effectieve bestrijdingsmiddelen tegen dit fenomeen.

71. Ook Bart Tommelein, senator voor Open VLD, onderkent de nood aan een aangescherpt beleid. Hij is dan ook vragende partij voor meer middelen voor de speurders van de Federal Computer Crime Unit, zodat ze kunnen optreden tegen de criminelen die opereren op het Darknet. In 2010 diende hij al een wetsvoorstel in, aangaande de handel in dopingproducten op het klassieke internet.[111] De criminaliteit die op Darknet welig tiert, is volgens Bart Tommelein echter nog een categorie erger. Tommelein stelde in de Senaat dan ook enkele schriftelijke vragen aangaande deze problematiek.[112] Hij benadrukt dat het hoognodig is om met de internetproviders samen te zitten en de mogelijkheden te bekijken. Tevens is hij een fervent voorstander om de middelen en de bevoegdheden van de Federal Computer Crime Unit significant op te schroeven. Infiltratie op het internet moet bespreekbaar worden, aldus Tommelein.[113]

[110] D. DECKMYN, "Speeltuin van wapenhandelaars en drugsdealers", *De Standaard* 4 maart 2012, (16) 16.
[111] Wetsvoorstel tot aanvulling van artikel 2 van de drugswet van 24 februari 1921 met het oog op de invoering van verzwarende omstandigheden in het kader van de handel van hormonale substanties voor menselijk gebruik, *Parl. St.* Senaat 2011-12, nr. 5-1274/1.
[112] Schriftelijke vraag van de heer Bart Tommelein tot de vice-eerste minister en minister van Financiën en Institutionele Hervormingen omtrent de website Silk Road, *Hand.* Senaat, 2011-12, 30 september 2011, nr. 5, 3296.
[113] D. DECKMYN, "De meerderheid wil gewoon kunnen facebooken", *De Standaard* 5 maart 2012, (6) 7.

DEEL IV: De aanpak van internationale organisaties inzake cybercriminaliteit

Hoofdstuk 1: Inleiding

72. Computercriminaliteit en de bestrijding ervan krijgt naarmate de tijd vordert steeds meer aandacht. Gezien cybercrime allerminst rekening houdt met landsgrenzen, zijn er tal van initiatieven ontstaan in de schoot van internationale organisaties. Deze internationale aanpak is broodnodig. Op nationaal niveau is er immers een te grote fixatie op het eigen nationale recht, en ontbreekt het aan een gecoördineerde aanpak van de problematiek. Dit blijkt eens te meer uit het feit dat de nationale wetgeving wereldwijd erg verschilt. Om die redenen is het aangewezen dat er via internationale fora wordt gezocht naar een efficiënte aanpak van cybercrime. In dit deel wordt er aandacht besteed aan deze initiatieven. Meer bepaald zullen de initiatieven van de OESO, de Verenigde Naties, de G8, de Europese Unie alsmede de Raad van Europa besproken worden.

Hoofdstuk 2: Aanpak van de OESO

73. De OESO is een organisatie die werd opgericht in 1961 en staat voor 'Organisatie voor Economische Samenwerking en Ontwikkeling'. De OESO heeft zijn hoofdzetel te Parijs en telt 34 leden, waaronder België. De organisatie heeft als doel het economische en sociale welzijn van mensen wereldwijd te verbeteren. De OESO biedt een forum voor overheden om ervaringen te delen en op zoek te gaan naar oplossingen voor gemeenschappelijke problemen.[114]

74. De OESO was de eerste internationale organisatie die richtlijnen opstelde in de strijd tegen cybercrime.[115] Niettemin is cybercrime vandaag de dag geen absolute prioriteit voor een instantie als de OESO. De organisatie focust meer op cyberveiligheid, en promoot een globaal gecoördineerde politionele aanpak. [116]

75. De eerste stappen vonden plaats tussen 1983 en 1985. Het ad hoc Committee on Computer Crime boog zich over de mogelijkheid om een internationale harmonisatie van het strafrecht door te voeren met betrekking tot computergerelateerde misdaad. Het comité deed

[114] http://www.oecd.org.
[115] Y.JEWKES en M. YAR, *Handbook of internet crime*, Devon, Willan Publishing, 2010, 401.
[116] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 8.

in dit kader dan ook de aanbeveling aan de lidstaten om na te gaan in welke mate ze deze vorm van criminaliteit in hun respectievelijke nationale wetgeving konden vatten. Vier jaar later kwam de OESO met de 'Recommendation concerning guidelines for the security of information systems'.[117][118] Met deze richtlijn had de OESO een implementatie van minimale beveiligingsmaatregelen voor informaticasystemen voor ogen. In 2003 werd er in Oslo de 'OESO Global Forum on Information Systems and Network Security' gehouden.[119] Samen met deze top vond er een workshop aangaande cybercrime plaats. De hierop volgende jaren werden er opnieuw bijeenkomsten georganiseerd, die gericht waren tegen de bestrijding van o.a. malware en spam.[120] In 2008 bracht de OESO een rapport uit genaamd 'Scoping paper on online identity theft'. In dit rapport maant de OESO haar leden aan adequate wetgeving te ontwikkelen om dit fenomeen te voorkomen, te detecteren en te bestrijden. Het rapport gaf tevens een weergave van de verschillende wetgevende initiatieven genomen door de OESO leden.[121] In 2009 publiceerde de OESO een boek met als titel 'Computer viruses and Other Malicious Software: A Threat to the Internet Economy'. De OESO hamert hierin op een beter wetgevend kader in de strijd tegen computercriminaliteit.[122]

Hoofdstuk 3: Aanpak van de VN

76. Ook de Verenigde Naties hebben meerdere initiatieven genomen inzake de strijd tegen internetcriminaliteit. Reeds in 1989 werd door de VN de 'Guidelines on the Use of Computerized personal Data Flow' aangenomen. In 1994 stonden de Verenigde Naties aan de wieg van de 'Manual on the prevention and control of computer-related crime'.[123] In 1997 werd in de schoot van de Verenigde Naties 'UNODC' opgericht. UNODC staat voor 'United

[117] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 393.
[118] Recommendation concerning guidelines for the security of information systems, 26 november 1992, www.oecd.org.
[119] www.cybercrimelaw.net/OECD.html.
[120] www.cybercrimelaw.net/OECD.html.
[121] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 393.
[122] OESO, *Computer viruses and Other Malicious Software: A Threat to the Internet Economy*, 2009, 244 p.
[123] N. KSHETRI, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, Londen, Springer, 2010, 19.

Nations Office on Drugs and Crime'. Het doel van het UNODC is de bestrijding van drugshandel en georganiseerde misdaad, waaronder cybercrime.[124]

77. In april 2000 vond te Wenen het 'Tenth United Nations Congress on the prevention of Crime and the Treatment of Offenders' plaats. De VN definieerde op dat moment cybercrime als volgt: "*Elk misdrijf dat kan gepleegd worden in een elektronische omgeving en waar men onder een misdrijf het vergrijp verstaat dat in het algemeen als onwettig wordt beschouwd of meestal wel gesanctioneerd wordt*."[125]

78. In datzelfde jaar vond er in Palermo, van 12 tot 15 december, een bijeenkomst plaats naar aanleiding van de ondertekening van de 'United Nations Convention against Transnational Organized Crime'. Gedurende deze bijeenkomst hield een specifiek panel, onder leiding van Hans Corell, zich bezig met 'The Challenge of Borderless Cybercrime'. De visie van de VN op het fenomeen cybercrime werd hoe langer hoe meer duidelijk. Op 29 maart 2001 vond in New York de 'Global InfoSec 2001 Conference' plaats. Afgevaardigden van de 189 leden van de VN bogen zich tijdens deze conferentie, samen met afgevaardigden van de Amerikaanse technologie-industrie, over het vraagstuk omtrent de aanpak van cybercrime. Het doel was om een coherente en globale strategie na te streven. De deelnemers aan de conferentie zagen het belang in van een internationaal wettelijk kader in de strijd tegen cybercrime. Niettemin was er tegenkanting vanuit de hoek van de Verenigde Staten, die soevereinrechtelijke problemen had met dergelijke aanpak. Het bleef met andere woorden bij vele goede bedoelingen en aanbevelingen, maar weinig concrete resultaten.[126] [127]

79. Op 11 november 2004 werk de 'Working Group on Internet Governance' opgericht.[128] Deze werkgroep had tot doel aanbevelingen te formuleren met het oog op een evenwichtig optreden van zowel private partijen als overheden. In 2010 lag het dossier aangaande internationale samenwerking in de strijd tegen cybercrime op de tafel van het 'Twelfth United Nations Congress on Crime Prevention and Criminal Justice'. Dit congres werd gehouden in Salvador, te Brazilië. Het hoofdzakelijke doel van dit congres bestond erin een strategie op te

[124] www.unodc.org/cybercrime-study.
[125] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 381.
[126] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 381.
[127] www.aitglobal.com/orgsite/events/InfoSec2001/un_infosec_2001.htm.
[128] Report of the Working group on Internet Governance, juni 2005, www.wgig.org.

bouwen voor de globale aanpak van criminele problemen. Het UNODC had, in voorbereiding van de top, een werkdocument opgesteld waarin werd gesuggereerd dat de ontwikkeling van een wereldwijde conventie tegen cybercrime moest worden overwogen.[129] [130] In enkele regionale meetings, voorafgaand aan de eigenlijke top, werd dit idee steeds meer leven ingeblazen. Vooral de Latijns-Amerikaanse landen steunden dit voorstel volop.[131] Het UNODC benadrukte de nood aan een globale aanpak, en meer bepaald de nood aan een internationale samenwerking in dit kader.[132] De organisatie stelde dat de snelheid waarmee cybercriminelen delicten plegen een enorme druk legt op politiële instanties, niet alleen wat betreft de opsporing zelf, ook wat betreft de detectie van nieuwe fenomenen. Verschillen in nationale wetgeving bemoeilijkt de opsporing van cybercriminelen alleen maar, convergentie is de sleutel tot succes.[133]

80. Het jaar 2010 had een mijlpaal kunnen worden in de strijd tegen cybercrime. Het VN congres in Brazilië bood namelijk opportuniteiten om onderhandelingen aan te gaan met als doel een wereldwijd verdrag inzake cybercrime. Tot op dat punt was het Cybercrime-Verdrag van de Raad van Europa immers de enige internationale tekst aangaande cybercrime. In 2010 bestond de mogelijkheid om hier een wereldwijde variant van op te stellen. Zover is het spijtig genoeg nooit gekomen. Er werd op het VN-congres gedurende tien dagen gedebatteerd over het voorstel, maar de onderhandelingen liepen met een sisser af. De Europese Unie en de Verenigde Staten zagen de noodzaak van een nieuw wereldwijd verdrag niet in, naar hun mening voldeed het Cybercrime-Verdrag van de Raad van Europa. De Verenigde Staten, net als het Verenigd Koninkrijk, wezen tevens op het feit dat het ontstaan van een verdrag in de schoot van de VN teveel voeten in de aarde zou hebben. Meer algemeen wierpen de EU, de VS en het UK ook argumenten op aangaande de problematiek van de soevereiniteit van de staat, evenals mensenrechtelijke bezwaren.[134] Zij stonden hiermee lijnrecht tegenover China, Rusland, en tal van ontwikkelingslanden.

---

[129] Working paper of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice (22 januari 2010), *UN Doc.* A/CONF.213/9 (2009), http://www.unodc.org.
[130] M. ERMERT, "Konkurrenz für Cybercrime-Konvention des Europarates", *Heise online* 18 maart 2010, www.heise.de.
[131] B. HARLEY, "A global Convention on Cybercrime?", *The Columbia Science and Technology Law review* 23 maart 2010, www.stlr.org.
[132] Background documents of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice (23 maart 2010), *UN Doc*. A/CONF.213 /IE/7, www.cybercrimelaw.net.
[133] B. HARLEY, "A global Convention on Cybercrime?", *The Columbia Science and Technology Law review* 23 maart 2010, www.stlr.org/2010/03/a-global-convention-on-cybercrime.
[134] G. MASTERS, "Global cybercrime treaty rejected at U.N.", *SC Magazine* 23 april 2010, www.scmagazine.com.

81. Ondanks deze gemiste horde blijft de VN bezig met de cybercrimeproblematiek. Zo kondigde Yury Fedotov, algemeen directeur van het UNODC, op 26 januari 2012 aan dat er een studie werd opgestart aangaande de problematiek van cybercrime en de acties die dienaangaande worden genomen door de lidstaten van de VN, de internationale gemeenschap en de private sector. De resultaten van deze studie zullen door de VN worden bekendgemaakt in 2013. [135] [136]

Hoofdstuk 4: Aanpak van de G8

82. Ook de G8 nam initiatieven inzake cybercrime. De G8, ook wel de groep van 8 genoemd, is een intergouvernementeel forum van acht vooraanstaande industriële grootmachten. De leden van de G8 zijn het UK, Frankrijk, Duitsland, Italië, Japan, Canada, Rusland en de VS. In 1975 zag de G6 het levenslicht, welke de G7 werd in 1978. Vanaf 1998 werd dit de G8, bestaande uit de G7 en Rusland. De G8 houdt jaarlijks een bijeenkomst, vooral gericht op economische en financiële problematieken. Ook politieke- en veiligheidsproblemen maken deel uit van de werkingssfeer.[137] Dat de G8 zich bezighoudt met cybercrime hoeft niet te verbazen. De leden van de G8 verliezen immers bergen geld door cybercriminaliteit.

83. De eerste stappen wat betreft cybercrime werden eind de jaren ’90 gezet. In 1997 werd een bijeenkomst over high-tech crime georganiseerd door de justitieministers van de P8. Vanaf de top van Napels in 1994, kwam de G7 na iedere topbijeenkomst bijeen met Rusland als de ‘politieke 8’, vandaar de term P8. [138] [139] Binnen de Lyon-Group werd er een ‘Subgroup on High-Tech Crime’ opgericht. [140] Deze groep houdt zich bezig met de strijd tegen cybercriminaliteit.[141]

[135] http://issat.dcaf.ch/Home/Community-of-Practice/Blogs/INPROL/UNODC-Study-on-Cybercrime.
[136] www.unodc.org/unodc/en/frontpage/2012/January/unodc-chief-announces-a-comprehensive-study-on-cybercrime.html.
[137] www.g8.utoronto.ca.
[138] G. VERMEULEN, *Wederzijdse rechtshulp in strafzaken in de Europese Unie: naar een volwaardige eigen rechtshulpruimte voor de Lid-Staten?*, Antwerpen, Maklu, 1999, 27.
[139] A. DEBAETS, J. DEENE en N. SENEL, “Cybercriminaliteit”, in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 387.
[140] J. R. WESTBY, *International Guide to Combating Cybercrime*, Chicago, American Bar Association, 2003, 67.
[141] N. KSHETRI, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, Londen, Springer, 2010, 19.

De P8 keurde op dat moment 10 principes goed:[142]

- "*there must be no safe havens for those who abuse information technologies;*
- *investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred;*
- *law enforcement personnel must be trained and equipped to address high-tech crimes;*
- *legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized;*
- *legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime;*
- *mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime;*
- *transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides;*
- *forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed en employed;*
- *to the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence;*
- *work in this area should be coordinated with the work of other relevant international for a to ensure against duplication of efforts."*

84. Ter ondersteuning van deze principes werd er eveneens een actieplan afgekondigd, bestaande uit 10 punten:[143] [144]

- *"use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis;*
- *take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other states;*

[142] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 387.
[143] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 387.
[144] Statement by attorney general Janet Reno on the meeting of justice and interior minister of the eight, 10 december 1997, www.fondazionefalcone.it.

- *review our legal systems to ensure and promote the investigation of high-tech crimes;*
- *consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements;*
- *continue to examine and develop workable solutions regarding the preservation of evidence prior to the execution of request for mutual assistance, transborder searches, and computer searches of data where the location of that data is unknown;*
- *develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally;*
- *work jointly with industry to ensure that the new technologies facilitate our effort to combat high-tech crime to preserving and collecting critical evidence;*
- *ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communication, including voice, fax, or e-mail, with written confirmation to follow where required;*
- *encourage internationally-recognized standards making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies;*
- *develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions."*

85. Begin mei van het jaar 2000 leerde de wereld het 'I Love You-virus' kennen.[145] Het virus werd het eerst gesignaleerd in Hong Kong, waarna het zich razendsnel verspreidde over de rest van de wereld. Zodra computergebruikers het bestand 'loveletter for you' openden, begon het virus zich onmiddellijk te verspreiden naar andere computers.[146] Het I Love You-virus werd op dat moment beschouwd als het gevaarlijkste virus ooit. De schade die het virus met zich meebracht was navenant, er werd gewag gemaakt van maar liefst 7 miljard dollar schade

[145] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 389.
[146] X., "Computers crashen wereldwijd door I Love You-virus", *Het Belang van Limburg* 5 mei 2000, www.hbvl.be.

wereldwijd.[147] [148]Onel de Guzman, een op de dag van de feiten 24-jarige Filipijnse student, werd beschouwd als zijnde de dader.[149] Vervolgd werd hij echter nooit, het Filipijnse ministerie van Justitie liet alle aanklachten vallen gezien deze geen betrekking hadden op het hacken van computers, en omdat de bewijslast niet zwaar genoeg was. Het grote probleem zat hem echter in het feit dat de Filipijnen kampten met een groot gebrek aan wetgeving.[150] Pas na de feiten werd er een wet aangenomen inzake computercriminaliteit, maar deze kon niet retroactief worden toegepast.[151]

86. Enkele weken na het uitbreken van het virus werd er een conferentie van de G8 georganiseerd in Parijs, met als thema het groeiende probleem van cybercrime. Toch is het I Love You-virus niet de enige reden waarom er werd overgaan tot een conferentie. De G8 wou zich tevens opmaken voor haar jaarlijkse bijeenkomst, later dat jaar, in Japan. Cybercrime stond daar namelijk ook als onderwerp op het programma. De leden van de G8 ondervonden zware hinder door het I Love You-virus. Ze wilden naar de toekomst toe dan ook proactieve maatregelen kunnen treffen om zich tegen dergelijke virusaanvallen beter te kunnen wapenen.[152] De G8 benadrukte tijdens deze conferentie de noodzaak van een doorgedreven dialoog tussen de overheid en de privésector.

87. De top van 24 juli 2000 in Japan legde opnieuw de nadruk op het ontwikkelen van maatregelen tegen cybercrime. De top versterkte in die zin de punten die reeds op de top in Parijs werden besproken.[153]

88. In oktober 2000 vond er een bijeenkomst plaats in Berlijn. De conferentie werd bijgewoond door tal van experten uit de sector en de overheid. Gezien het moeilijk was het

[147] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 389.
[148] J. BIESEMANS, "G8-landen vergaderen over cybermisdaad", *ZDNet België* 15 mei 2000, www.zdnet.be.
[149] X., "Verdachte maker 'I Love You'-virus niet vervolgd", *Webwereld* 21 augustus 2000, www. webwereld.nl.
[150] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 389.
[151] X., "Verdachte maker 'I Love You'-virus niet vervolgd", *Webwereld* 21 augustus 2000, www.webwereld.nl.
[152] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 389.
[153] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 390.

eens te worden over algemene normen, legde men zich toe op de technische aspecten van het probleem. Formele afspraken werden er echter niet gemaakt.[154]

89. Een volgende horde werd genomen in februari 2001, op een top van de ministers van Justitie en Binnenlandse Zaken, in Milaan.[155] Tijdens deze conferentie werd er vooral een focus gelegd op het tegengaan van de seksuele uitbuiting van minderjarigen.[156] Tevens werd het startschot gegeven voor een wereldwijde campagne tegen cybercriminaliteit. Verder werd er besloten over te gaan tot de oprichting van een G8-database, waarin de verschillende landen relevante informatie omtrent cybercriminelen zouden samenbrengen.

90. Echte progressie met betrekking tot de uitvoering van een actieplan tegen cybercrime werd er bereikt tijdens de 'High-Tech Crime Meeting' van mei 2001, te Tokio.[157] In werkgroepen wisselden experten gedachten uit over dataretentie, databewaargeving, elektronische handel en gebruikersauthenticiteit en training.[158]

91. In mei 2004 vond er te Washington D.C. een nieuwe G8-top plaats van de ministers van Justitie en Binnenlandse Zaken.[159] Tijdens deze conventie scharen zij zich achter het initiatief voor een brede wetgeving, zoals voorzien in het Cybercrime-Verdrag van de Raad van Europa, dat een maand later in werking zou treden. Het communiqué stelde in dit kader: *"To truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations. With the Council of Europe's Convention on Cybercrime coming into force on July 1, 2004, we should take steps to encourage the adoption of the legal standards it contains on a broad basis"*

92. Nog geen 2 jaar later vond er in Moskou een nieuwe top plaats van de ministers van Justitie en Binnenlandse Zaken.[160] Hier bevestigden en versterkten zij hun standpunten van de

[154] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 390.
[155] www.g8.utoronto.ca/evaluations/2001genoa/objectives/crimes.html.
[156] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 391.
[157] G8 Conference on High-Tech Crime, 22-24 May 2001, Tokyo, www.statewatch.org.
[158] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 392.
[159] www.g8.utoronto.ca/foreign/.
[160] www.g8.utoronto.ca/foreign/.

top van 2004: "*We also discussed issues related to sharing accumulated international experience in combating terrorism, as well as comparative analysis of relevant pieces of legislation on that score. We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that it is necessary to device a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors."*

93. In 2009 ontmoeten de ministers van Justitie en Binnenlandse Zaken elkaar opnieuw, ditmaal in Rome. Gedurende deze top voerden zij gesprekken over de strijd tegen internetpiraterij, en cybercriminaliteit in het algemeen.[161]

94. In 2011 vond er een top plaats in Deauville, met cyber security als één van de prioritaire onderwerpen.[162] [163] Het doel was de toegang tot internet te verbeteren, het recht op vrijheid van meningsuiting te ondersteunen, de veiligheid op internet te vergroten en bescherming te bieden aan individuen.[164]

Hoofdstuk 5: Aanpak van de Raad van Europa

1. INLEIDING

95. De Raad van Europa is de oudste Europese organisatie, en zag het levenslicht op 5 mei 1949, wanneer hij door 10 staten werd opgericht. Ondertussen telt de Raad van Europa reeds 47 lidstaten, waaronder België. Hierdoor beslaat de werkingssfeer van de Raad van Europa

[161] G8 Justice and Home Affairs Ministers' Declaration on The Fight Against Piracy, 30 mei 2009, Rome, www.canadainternational.gc.ca.
[162] G8 Final Declaration concerning Internet, 26 mei 2011, Deauville, www.g7.utoronto.ca.
[163] G8 Preparatory Plans for the 2011 G8 Deauville Summit, 26-27 mei 2011, Deauville, www.g8.utoronto.ca.
[164] G8 Preparatory Plans for the 2011 G8 Deauville Summit, 26-27 mei 2011, Deauville, www.g8.utoronto.ca.

nagenoeg het hele Europese continent. De organisatie heeft haar zetel in Straatsburg, en heeft tot doel de democratie, mensenrechten en de naleving van rechtsregels in de lidstaten te versterken.[165]

96. De Raad van Europa speelt inzake cybercriminaliteit een zeer grote rol, in die zin dat in haar schoot het Cybercrime-Verdrag is ontstaan. Datzelfde Cybercrime-Verdrag was het eerste, en tot op heden, het enige internationale verdrag gericht op de bestrijding van cybercriminaliteit.[166]

97. Het verdrag bevat vanzelfsprekend, zoals hierna besproken zal worden, een lijst met informaticagerelateerde misdrijven. Toch valt er hieromtrent een significante hiaat op te merken, waarop ik reeds nu al even uw aandacht wil vestigen. Bij de totstandkoming van het verdrag werd er immers geen overeenstemming bereikt over een bepaling omtrent rassenhaat.[167] Het was daarentegen initieel wel de bedoeling inhoudsgebonden misdrijven in de verdragstekst op te nemen. Met inhoudsgebonden misdrijven werd gedoeld op strafbare bepalingen aangaande kinderpornografie en rassenhaat. De voornaamste reden waarom de verdragstekst geen bepalingen bevat omtrent het aanzetten tot raciale haat, in tegenstelling tot kinderpornografie, dienen we bij de Verenigde Staten te zoeken.[168] De VS weigerde immers een verbod op racistisch materiaal in te stellen, ondanks de uitdrukkelijke wens van de Europese landen om racistische websites op dezelfde manier te verbieden als kinderpornografie. De reden voor deze weigering lag hem in het gegeven dat de Verenigde Staten meenden dat een dergelijk verbod zou indruisen tegen het Eerste Amendement van de Amerikaanse grondwet. Dit Eerste Amendement waarborgt de vrije meningsuiting. Er ontstond op dat punt een aanzienlijke impasse, met het risico dat het hele initiatief in het water zou vallen. Gezien de grote belangen die op het spel stonden, werd er overgegaan tot compromis. De bepalingen omtrent racistisch materiaal werden uit het verdrag geweerd, en werden opgenomen in een aanvullend protocol. Dat aanvullend protocol, dat tot stand kwam

[165] www.coe.int.
[166] J. CLOUGH, *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 22.
[167] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 397.
[168] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 398.

op 28 januari 2003, voorzag dat elke verspreiding van racistische of xenofobische propaganda via computernetwerken een strafrechtelijk misdrijf werd.[169]

98. In de hierop volgende punten zal zowel de ontstaansgeschiedenis, als de inhoud van het Cybercrime-Verdrag worden besproken, evenals het aanvullend protocol van 2003 en het kaderbesluit van 2005.

2. ONTSTAANSGESCHIEDENIS VAN HET CYBERCRIME-VERDRAG

99. De komst van het Cybercrime-Verdrag van de Raad van Europa op 23 november 2001 was in elk opzicht een mijlpaal. 2001 was in dat opzicht een belangrijk jaar inzake de strijd tegen cybercriminaliteit. De voorbereidingen naar dit orgelpunt startten echter veel vroeger.

100. Reeds eind de jaren '80 begon de Raad van Europa aandacht te besteden aan criminaliteit met betrekking tot nieuwe technologieën. In 1989 kwam de Raad van Europa met een eerste aanbevelingen aangaande computergerelateerde misdaad.[170] De zogenaamde 'Recommandation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime' kwam er na intensief werk van het 'Select Committee of Experts on Computer-Related Crime'. Recommendation No. R (89) 9 was erop gericht lidstaten ertoe te brengen om bij eigen wetgevende initiatieven rekening te houden met het rapport aangaande computergerelateerde misdaad.[171] [172] In laatstgenoemd rapport wordt een minimumlijst voorgesteld, die lidstaten kunnen gebruiken als richtlijn in het kader van het strafbaar stellen van vormen van cybercriminaliteit.[173] Deze minimumlijst is een verdere evolutie van de lijst van de OESO, naast deze minimumlijst werd ook een optionele lijst opgesteld.

[169] Additional Protocol to the Convention on Cybercrime Council of Europe ETS no. 189, 2003, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg.
[170] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 398.
[171] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 399.
[172] Recommendation Council of Europe No. R (89) 9 adopted by the Committee of Ministers of the Council of Europe, 13 september 1989, concerning Computer-Related Crime.
[173] Recommendation Council of Europe No. R (89) 9, 1990, on computer-related crime and final report of the European Committee on Crime Problems, Strasbourg. www.oas.org.

101. Op 8 september 1995 volgde een nieuwe aanbeveling van de Raad van Europa, aangaande de opsporing van strafbare feiten in een geautomatiseerde omgeving. [174] Recommendation No. R (95) 13 kan als opvolger worden beschouwd van recommendation No. R (89) 9. De aanbeveling van september 1995 bevat een aantal krachtlijnen die tot nut kunnen zijn voor de leden van de Raad van Europa.[175] De principes van de aanbeveling zijn vooral gericht op een aantal nieuwe, specifieke bevoegdheden van politie en justitie. Het gaat onder meer over het gebruik van cryptografie en elektronisch bewijs, onderzoek, training en statistiek, evenals de verplichting om medewerking te verlenen en ook internationaal samen te werken.[176] Het uitgangspunt was om deze principes over te nemen in bestaande nationale wetgeving. Niettemin heeft deze recommandation, net als de recommandation van 1989, geen bindende kracht.[177] Beiden roepen de lidstaten op om de conclusies over te nemen en om te zetten in hun eigen wetgeving. Of deze lidstaten dat ook effectief doen, is hun eigen keuze.

102. In februari 1997 werd er in de schoot van het comité van ministers van de Raad van Europa een ad hoc comité van experten opgericht. Dit comité, dat de naam 'Committee of experts on Crime in Cyberspace (PC-CY)' kreeg, stond onder leiding van H.W.K. Kaspersen. [178] Het doel van dit comité bestond erin onderzoek te verrichten naar cybercriminaliteit, te kijken welke wetgeving geharmoniseerd moest worden, alsook onderzoek voeren naar de interceptie van telecommunicatie en de elektronische observatie van informatienetwerken.[179] Naast deze algemene doelstellingen diende het comité zich ook toe te leggen op het onderzoek naar de mogelijkheid om websites te doorzoeken en materiaal ervan in beslag te nemen.[180] Ook diende er nagegaan te worden op welke wijze er effectief kon worden samengewerkt op internationaal gebied, en welke verplichtingen men aan internetproviders kon opleggen.[181] [182] Het einddoel was dat men aan de hand van al deze bevindingen een verdrag kon opstellen,

[174] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 399.
[175] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 91.
[176] P. VAN EECKE, *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 92.
[177] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 398.
[178] Henrik W.K. Kaspersen is hoogleraar-directeur van het Computer/Law Institute van de Vrije Universiteit te Amsterdam.
[179] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 399.
[180] F. KUITENBROUWER, "Verdrag crime in cyberspace", *Computerr.* 2000, (116) 116.
[181] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 399.
[182] H.W.K. KASPERSEN, "Voortgang van het Cybercrimeverdrag", *Computerr.* 2001, (105) 105.

met zowel materieel- als formeelrechtelijke bepalingen aangaande cybercriminaliteit, dat bindend was voor alle lidstaten van de Raad van Europa.[183]

103. Op 27 april 2000 heeft het PC-CY de ontwerptekst van het Cybercrime-Verdrag voorgesteld. Dat dit ontwerp werd vrijgegeven was enigszins ongebruikelijk, maar had een duidelijk doel. Op deze wijze konden experten de draft inkijken en commentaar aangaande het ontwerp formuleren.[184] Een jaar later, op 6 maart 2001, werden experten van over de hele wereld uitgenodigd op een speciale hoorzitting georganiseerd door de parlementaire Assemblee van de Raad van Europa. Tijdens deze hoorzitting werden bezwaren aangaande de ontwerptekst aanhoord.[185]

104. Op 19 september 2001 werd het Cybercrime-Verdrag goedgekeurd door de afgevaardigde ministers van de Raad van Europa. Op 8 november van datzelfde jaar werd het verdrag voorgesteld voor een formele aanneming. Na jarenlange voorbereidingen volgde het orgelpunt op 23 november 2001, wanneer het verdrag officieel werd opengesteld voor ondertekening op een internationale conferentie te Budapest.[186] [187]

105. Tot op heden werd het Cybercrime-Verdrag door 47 landen ondertekend, en door 33 landen geratificeerd.[188] Het verdrag zou in werking treden als 5 staten, waarvan er tenminste 3 lid zijn van de Raad van Europa, het geratificeerd hadden. Deze drempel werd bereikt op 1 juli 2004.

106. Wat deze cijfers betreft zijn er vier markante zaken vast te stellen. Als we in het achterhoofd houden dat het doel was een optreden te garanderen dat zorgt voor een breed Europees draagvlak tegen cybercrime, vallen volgende zaken op. Eerst en vooral is het opvallend dat niet alle lidstaten van de Raad van Europa het verdrag hebben ondertekend. Zo

[183] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 399.
[184] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 399.
[185] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 399.
[186] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 399.
[187] Convention on cybercrime Council of Europe ETS no. 185, 2001. Budapest.
[188] http://conventions.coe.int/Treaty/.

vinden we Andorra, Monaco, Rusland en San Marino terug in de lijst van niet-ondertekenaars.[189]

107. Een tweede opvallend aspect zit hem in het feit dat ook niet-lidstaten van de Europese Raad het verdrag hebben ondertekend, zoals de Verenigde Staten, Canada, Japan en Zuid-Afrika. Ook organisaties als de EU, de OESO en de UNESCO waren nauw bij het verdragwerk betrokken. [190]Op deze wijze gaat de Raad van Europa dus verder dan het eerst vooropgestelde Europese draagvlak. Dit impliceert tevens dat cybercriminelen buiten Europa kunnen worden vervolgd. Een derde opvallend feit situeert zich in de Belgische situatie. België ondertekende namelijk het verdrag op 23 november 2001, maar is tot op vandaag nog niet overgegaan tot ratificatie. Guido De Padt stelde op 26 mei 2011, omtrent dit gegeven, in de senaat een schriftelijke vraag aan de minister van Justitie. Een laatste opvallend aspect is de hoeveelheid van landen die het verdrag ondertussen heeft getekend en geratificeerd. Maar liefst 47 landen ondertekenden het verdrag, 33 van hen gingen intussen reeds over tot ratificatie. Dit is, gezien de meeste verdragen in het beste geval ondertekend worden door 10 tot 20 landen, een sterke prestatie.[191] Dergelijk enthousiasme valt in dit kader wel te verduidelijken. Cybercrime is immers een wereldwijde problematiek. Daarenboven onderkennen vele landen de nood aan een uniforme regelgeving, en laat het verdrag ook ruimte voor beoordelingsvrijheid aan de lidstaten.[192]

3. BESPREKING VAN HET CYBERCRIME-VERDRAG

3.1 Doelstellingen

108. Bij de ondertekening van het Cybercrime-Verdrag op 23 november 2001, stonden drie doelstellingen voorop. Deze doelstellingen worden weerspiegeld in de structuur van het verdrag.

[189] http://conventions.coe.int/Treaty/.
[190] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 397.
[191] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 397.
[192] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.

109. Eerst en vooral wordt er nadruk gelegd op de harmonisering van het materiële strafrecht wat betreft de zogenaamde specifieke informaticamisdrijven. Er worden gemeenschappelijke definities vastgelegd van bepaalde strafrechtelijke inbreuken, wat als gevolg heeft dat harmonisatie van nationale wetten mogelijk wordt. Dit alles heeft tot doel om het ontstaan van zogenaamde 'data havens'[193] in te perken en te bestrijden.[194]

110. Een tweede doelstelling kadert in de strafrechtprocedure. Met name wordt er gepoogd harmonisatie van opsporingsbevoegdheden in relatie tot computersystemen en -netwerken na te streven.[195] Het verdrag bevat bepalingen omtrent methodes voor strafrechtelijk onderzoek en vervolging, met het oog op het op elkaar afstemmen van nationale strafrechtelijke procedures. Op deze wijze wil men opnieuw het ontstaan van 'data havens' voorkomen, in het geval dat bepaalde inbreuken door de ene verdragspartij zouden kunnen worden opgespoord, maar door een andere niet.[196]

111. Tenslotte bestaat de laatste doelstelling erin een regeling voor rechtsmacht te ontwikkelen, in het geval dat de cybercriminaliteit een internationale dimensie heeft.[197]Deze laatste doelstelling zou men als de belangrijkste kunnen beschouwen.[198] Cybercriminaliteit is immers een fenomeen dat landsgrenzen overschrijdt, het is dan ook noodzakelijk om in dit kader regels vast te leggen omtrent het bevorderen van internationale rechtshulp.

3.2 Summiere artikelsgewijze bespreking

112. Het Cybercrime-Verdrag telt 4 grote chapters of hoofdstukken. Het eerste hoofdstuk legt enkele belangrijke definities vast. Het tweede hoofdstuk is gewijd aan de maatregelen die op het nationale niveau dienen genomen te worden. Het derde hoofdstuk betreft regels omtrent de internationale samenwerking. Het vierde hoofdstuk, tenslotte, behelst enkele finale

[193] Data havens zijn een toevluchtsoord voor ongereglementeerde data, vaak in landen met een soepele informaticawetgeving. Ze maken het criminelen mogelijk activiteiten uit te oefenen in een staat waar deze niet strafbaar zijn. Het is vergelijkbaar met een het gegeven van een belastingsparadijs in fiscale aangelegenheden.
[194] P. VAN EECKE, "COLUMN. Criminaliteit in cyberspace", *De Standaard Online* 26 november 2001, www.standaard.be.
[195] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (433) 425.
[196] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 400.
[197] P. VAN EECKE, "COLUMN. Criminaliteit in cyberspace", *De Standaard Online* 26 november 2001, www.standaard.be.
[198] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 400.

bepalingen, zoals de ondertekening en inwerkingtreding, de toetreding en de territoriale werkingssfeer. Deze vier onderdelen zullen hierna kort besproken worden.

3.2.1 Definities

113. Het Cybercrime-Verdrag definieert in Artikel 1 vier begrippen, met name 'computersysteem', 'computergegevens', 'dienstverlener' en 'verkeersgegevens'. Elk van deze vier begrippen is in het verdrag ruim geformuleerd.[199]

3.2.2 Maatregelen op nationaal niveau

114. In hoofdstuk 2 van het Cybercrime-Verdrag worden de maatregelen besproken die moeten worden genomen op nationaal niveau. Het hoofdstuk valt uiteen in drie secties.

3.2.2.1 Materieel strafrecht

115. De eerste sectie handelt over een reeks strafbaarstellingen die de ondertekenende staten in hun wetgeving dienen op te nemen.

- *Titel 1, Artikel 2 tot 6: misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van computersystemen en -gegevens.*

  In deze categorie worden de specifieke informaticamisdrijven besproken, zoals deze al eerder in dit werk aan bod kwamen. De ondertekenende staten dienen deze inbreuken strafbaar te stellen in hun eigen nationale wetgeving, om zo een zekere harmonisatie na te kunnen streven. De desbetreffende inbreuken zijn de volgende: onwettige toegang, onwettige onderschepping, datamanipulatie, systeemmanipulatie en misbruik van toestellen. Artikel 2 heeft betrekking op de opzettelijke wederrechtelijke toegang tot een systeem. Dit dient strafbaar gesteld te worden. Er wordt hier vooral gedoeld op het fenomeen 'hacking'.[200] Artikel 3 wil optreden tegen het afluisteren van gegevensverkeer, gaande via telecommunicatie naar of afkomstig van een computersysteem.[201] Artikel 4 bestraft de opzettelijke wederrechtelijke beschadiging, wijziging, weglating of vernietiging

[199] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[200] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[201] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 401.

van geautomatiseerde opgeslagen gegevens. Artikel 5 heeft tot doel gedragingen te bestraffen die storingen teweegbrengen in het functioneren van een computersysteem. Hierbij wordt uitdrukkelijk gedoeld op computervirussen.[202] Artikel 6 is een meer algemene bepaling. Deze stelt dat het vervaardigen, beschikbaar stellen en verspreiden van instrumenten die de inbreuken in de artikelen 1 tot 5 mogelijk maken, strafbaar moet gesteld worden. Concreet betreft het software die voorafgaande inbreuken mogelijk kan maken.[203] Opmerkelijk hierbij is wel dat het verdrag expliciet bepaalt dat deze programma's met een misdadig oogmerk moeten worden gemaakt, net om inbreuken te plegen.

- *Titel 2, Artikel 7 en 8: computergerelateerde misdrijven*

  In tegenstelling tot titel 1, vormt het computersysteem hier naast het constitutief bestanddeel ook de modus operandi van het misdrijf. Concreet betreft het computergerelateerde valsheid en bedrog.[204]

- *Titel 3, Artikel 9: inhoudsgebonden misdrijven*

  Deze titel is volledig gewijd aan kinderpornografie. Het verdrag stelt het maken, aanbieden, verspreiden, verwerven en bezitten van kinderporno strafbaar. Artikel 9 bepaald tevens wat er nu juist onder kinderpornografie dient te worden verstaan. Concreet dient het te gaan over een minderjarige, of een persoon die als minderjarig wordt aanschouwd, die expliciete seksuele handelingen stelt. Opvallend is ook dat het verdrag het heeft over een realistische uitbeelding van een kind. Computeranimaties, met name virtuele kinderpornografie, en dergelijke meer vallen dus ook onder het toepassingsgebied.[205] Algemeen wordt een leeftijdsgrens bepaald van 18 jaar in de beschouwing van wat onder minderjarigheid dient te worden verstaan, al bepaalt het verdrag dat landen zelf een leeftijdslimiet vaststellen, al mag deze niet lager zijn dan 16 jaar. Initieel was het de bedoeling om in deze titel ook een bepaling op te nemen omtrent de verspreiding van rassenhaat. Deze bepaling kwam er door Amerikaanse druk echter niet, zoals al eerder werd vermeld.

[202] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[203] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[204] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 402.
[205] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 402.

- *Titel 4, Artikel 10: misdrijven verbonden aan inbreuken op het auteursrecht en verwante rechten*

  Auteursrechten laten naleven op het internet is een erg moeilijk en delicaat gegeven. Toch doet het Cybercrime-Verdrag een poging om een zekere context aan te bieden in artikel 10. Hoe dan ook blijven er manifeste problemen bestaan.[206] Vooreerst bleek het onmogelijk om in een Europese context een geüniformeerd stelsel van auteursrechten te ontwikkelen. Gezien er naast EU-landen ook niet-EU-landen het verdrag ondertekenden ontstaat er een lappendeken van verschillende auteursrechtelijke wetgeving. Hans Graux maakt op dit punt dan ook een terechte opmerking in die zin dat men zich de vraag kan stellen of het wel wenselijk is auteursrechtelijke inbreuken te regelen, als men het onderling al niet eens kan worden over welke handelingen nu juist inbreuken op het auteursrecht uitmaken. [207]

- *Titel 5, Artikel 11, 12 en 13: accessoire aansprakelijkheid*

  Artikelen 11 en 12 zijn gewijd aan de aansprakelijkheid die kan voortvloeien uit de voorafgaande misdrijven. Artikel 11 behandelt de strafrechtelijke poging en de medeplichtigheid. Artikel 12 behelst de strafrechtelijke aansprakelijkheid van rechtspersonen. Artikel 13 behandelt het sanctieregime.

3.2.2.2 Strafprocesrecht

116. De tweede sectie van het tweede hoofdstuk van het Cybercrime-Verdrag behandelt procesrechtelijke bepalingen. Deze zijn van belang omdat ze tot doel hebben een efficiënte opsporing en vervolging mogelijk te maken ten aanzien van cybercriminaliteit.

117. In artikel 14 en 15 worden voorwaarden en beschermingsmechanismen vastgelegd die van toepassing zijn op de volledige sectie.

118. Artikel 16 en 17 zijn erop gericht een verplichting in te voeren voor de ondertekenende staten om het opslagen van computergegevens mogelijk te maken. Dit is als het ware een bevriezingsmaatregel, waarmee een staat zich kan wapenen tegen de vluchtigheid van het

[206] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[207] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.

internet.[208] Artikel 17 is de meest specifieke van de twee, deze handelt immers over verkeersgegevens, waar artikel 16 computergegevens in het algemeen als onderwerp heeft.[209]

119. Artikel 18 roept een overleggingsbevel in het leven. Op deze manier poogt het Cybercrime-Verdrag onwillige systeembeheerders buiten spel te zetten. Een situatie waarbij een systeembeheerder weigert toegang tot zijn systeem te verschaffen, met als gevolg dat de inbeslaggenomen data ontoegankelijk worden, is niet ondenkbaar. Via artikel 18 wordt de ondertekenende staten opgelegd een regeling in hun nationale wetgeving op te nemen die het mogelijk maakt om bepaalde personen of instanties te bevelen de nodige gegevens aan het daglicht te brengen.[210]

120. Artikel 19 van het Cybercrime-Verdrag regelt de inbeslagneming en doorzoeking van informaticasystemen. De klassieke figuur van het beslag kampt in het kader van cybercriminaliteit met enkele praktische problemen. Onder de klassieke regelgeving zou men immers gehele computers, of in elk geval de gebruikte opslagmedia, in beslag moeten nemen. Niet alleen is deze werkwijze niet bepaald efficiënt, ze past eveneens niet in de figuur van het beslag. Het beslag kan immers enkel toegepast worden op roerende goederen, iets waaronder men computerdata bezwaarlijk kan thuisbrengen.[211] Artikel 19 wil in dit opzicht dan ook een oplossing bieden door de doorzoeking van individuele systemen en netwerken mogelijk te maken. De gegevens die men dan zou aantreffen kan men meenemen door inbeslagname.[212]

121. Artikel 20 en 21 voorzien in de onderschepping van computergegevens, en dit in real-time. Artikel 20 behelst enkel de verkeersgegevens, waar artikel 21 ook in de interceptie van inhoudelijke gegevens voorziet.

122. Het globale doel dat deze sectie dus nastreeft is het vergemakkelijken van strafrechtelijke onderzoeken in cyberspace. De politie krijgt in dit kader dan ook meer uitgebreide bevoegdheden om computerapparatuur in beslag te nemen en in netwerken binnen te dringen.[213]

[208] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[209] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[210] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[211] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[212] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[213] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 403.

3.2.2.3 Rechtsmacht

123. De derde, en laatste, sectie van dit hoofdstuk behandelt de rechtsmacht. Deze materie komt in het verdrag maar summier aan bod. Op het eerste zicht lijkt dit enigszins vreemd, rechtsmacht is een belangrijk aspect van een coherente aanpak van cybercriminaliteit. Toch dient het summiere karakter van artikel 22 niet te verbazen. In het Europees kader bestaan er immers al andere normatieve teksten die strekken tot het regelen van de rechtsmacht.[214] Indien de Raad van Europa had geopteerd voor een uitgebreide regulering, bestond er namelijk een aanzienlijke kans op overlappingen en daarbij horende problemen.[215] Meer specifiek stelt artikel 22 de verplichting in naar de ondertekende landen om een jurisdictie in te stellen voor misdrijven gepleegd op hun grondgebied, of gepleegd door een onderdaan.

3.2.3 Internationale samenwerking

124. Het derde hoofdstuk van het Cybercrime-Verdrag handelt over internationale samenwerking. Aan dit onderdeel wordt meer waarde geschonken dan aan rechtsmacht, wat blijkt uit de omvangrijke omschrijving in de 6 artikels. Het hoofdstuk valt uiteen in een sectie met algemene beginselen, en een sectie met specifieke voorzieningen. Het behandelt, algemeen beschouwd, de traditionele wederzijdse rechtshulp in twee modaliteiten. Enerzijds, het geval waarin er een legale basis bestaat tussen de partijen en, anderzijds, wanneer dit niet het geval is.[216] [217]

3.2.3.1 Algemene beginselen van internationale samenwerking

125. De algemene beginselen bespreken de te respecteren grondregels in de onderliggende verhoudingen tussen de verdragstaten. Artikel 23 legt de nadruk op de algemene principes van de uitvoering en de samenwerking te goeder trouw. De hierop volgende artikels gaan dieper in op enkele meer specifieke principes.[218]

[214] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[215] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[216] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 403.
[217] Explanatory report on the Convention on cybercrime Council of Europe ETS no. 185, 16 december 2001.
[218] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.

126. Artikel 24 behelst de uitlevering van criminelen. Belangrijke kanttekening bij dit artikel is dat het enkel toepasselijk is indien het misdrijf in beide landen strafbaar is gesteld met een gevangenisstraf van 1 jaar of meer.

127. Artikel 25 behandelt het principe van de wederzijdse bijstand. Dit artikel is meer praktisch van aard, in die zin dat het bepaalt op welke manier aanvragen tot informatie dienen te geschieden, en op welke wijze de afhandeling van dergelijke verzoeken dient te gebeuren.

128. Artikel 26 bevindt zich ook in de sfeer van de wederzijdse bijstand. Dit artikel laat de verdragspartijen toe om elkaar onderling, ongevraagd en spontaan, informatie aan te reiken. Dit kan geschieden wanneer de gevraagde partij de mening is toegedaan dat dit een onderzoek bij de vragende partij zou kunnen vergemakkelijken of versnellen.

129. Artikel 27 en 28 voorzien in een gedetailleerde samenwerkingsprocedure, die de verdragstaten kunnen hanteren indien zij zelf geen uitgewerkte procedure voorhanden hebben.

3.2.3.2 Specifieke voorzieningen in het kader van internationale samenwerking

130. De specifieke voorzieningen worden behandeld in de artikelen 29 tot en met 35. In deze artikelen wordt de samenwerking besproken in enkele specifieke situaties.

131. De artikel 29 en 30 handelen over het geval waarin doelgegevens zich bevinden op een systeem in een ander land. In dergelijk geval kan men beroep doen op de samenwerkingsprocedure, zoals voorzien in het verdrag. Om hiertoe over te gaan dient dit ander land wel het Cybercrime-Verdrag te hebben ondertekend.

132. Artikel 31 is, wat de situatieschets betreft, vergelijkbaar met de artikelen 29 en 30. Alleen betreft het hier wederzijdse rechtshulp, voor data die zich bevinden in een andere verdragsstaat.

133. Artikel 32 laat grensoverschrijdende toegang tot computerdata toe, zonder de toestemming van een andere verdragspartij. Dit indien de data voor het publiek toegankelijk zijn, of indien het een computersysteem betreft dat zich op het eigen grondgebied bevindt, maar de opgeslagen data in een andere verdragsstaat.

134. Artikelen 33 en 34 behandelen de mogelijkheid tot het verschaffen van toegang tot opgeslagen computergegevens, en maken tevens wederzijdse bijstand mogelijk bij het verkrijgen van verkeers- en inhoudsgegevens.[219]

135. Artikel 35 heeft betrekking op het mogelijk maken van snelle samenwerking door het opzetten van contactpunten.[220] Hiermee wordt enigszins tegemoetgekomen aan het gebrek aan echte grensoverschrijdende computerzoekingen. In elk van de ondertekenende staten wordt een contactpunt opgestart dat 24 uur op 24, 7 dagen op 7, beschikbaar is. Op deze manier wou men een vlotte communicatie bekomen tussen de verschillende verdragstaten, waardoor men sneller en efficiënter kan optreden tegen grensoverschrijdende cybercriminaliteit.[221]

3.2.4 Slotbepalingen

136. Het vierde en laatste hoofdstuk van het verdrag bevat enkele bepalingen omtrent de ondertekening en inwerkingtreding, de toetreding tot het verdrag, evenals de territoriale werkingssfeer.

3.3 Een kritische invalshoek

137. Het Cybercrime-Verdrag laat niemand onberoerd. Het lokte tal van positieve, maar ook negatieve reacties uit. Deze negatieve reacties kwamen uit verschillende hoeken. De algemene teneur in dit kader werd mooi verwoord door Jason Mahler, hoofd van de CCIA.[222] Hij stelde dat *"The intentions behind the treaty are valid, but as the first draft came out, it seemed to raise more problems than it would cure"*.[223] Enkele vaak gehoorde kritieken zullen hierna besproken worden.

138. Vooreerst is er de kritiek op artikel 6 van het Cybercrime-Verdrag, komende van beveiligingsdeskundigen. Artikel 6 bepaalt dat het vervaardigen, beschikbaar stellen en

[219] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (433) 464.
[220] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 403.
[221] H. GRAUX, "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.
[222] CCIA staat voor Computer & Communications Industry Association. De CCIA is een non-profit organisatie die open markten, open systemen, open netwerken en open concurrentie wil bevorderen.
[223] X., "Cybercrime treaty raises privacy concerns", *ZDNet* 13 oktober 2000, www.zdnet.com.

verspreiden van instrumenten die de inbreuken in de artikelen 1 tot 5 mogelijk maken, strafbaar moet worden gesteld. Deze bepaling lokte sterke reacties uit, omdat de bepaling zo ruim zou zijn dat ook sommige beveiligingssoftware kan worden verboden.[224] Dit heeft als ongewenst effect dat het voor programmeurs onmogelijk zou worden hun software te testen, en dat zij als hackers zouden worden aanzien. De GILC[225] steunt deze opvatting, door te stellen dat de term "illegale middelen" te weinig is gespecifieerd in het verdrag.[226] De vraag is echter of deze kritiek wel terecht is. H.W.K Kaspersen stelt in dit opzicht dat het verdrag allerminst de bedoeling heeft om het testen van computerbeveiliging, wat legaal is, te verbieden. Daden die gemachtigd zijn en uitgevoerd worden door diensten van de staat, of die vallen onder wettelijke commerciële praktijken vallen niet onder het verbod.[227]

139. Een andere vaak gehoorde kritiek is gericht op de afwezigheid van een bepaling omtrent het aanzetten tot racisme. Deze kritiek is eerder terecht. Ondanks het feit dat er voor een tussenoplossing werd gekozen via het aanvullend protocol, blijft het een lacune in het Cybercrime-Verdrag. Ik kan mij niet van de indruk ontdoen dat, ten tijde van de opstelling van het verdrag, de steun van de Verenigde Staten broodnodig was om het Cybercrime-Verdrag wat meer cachet te geven. Op zich is dit geen laakbaar gegeven, de VS is en blijft een belangrijke partner, maar toch is deze hele historie een teken aan de wand wat betreft de relaties tussen de EU-landen en de VS. Er bestaat geen twijfel dat binnen deze relaties, de VS de lakens uitdeelt. Het valt dan ook te betreuren dat de Raad van Europa haar wil niet heeft kunnen doordrukken, en voor een, als u wil, compromis à la Belge heeft geopteerd.

140. Een andere kritiek, die vooral werd geuit door groeperingen ter bescherming van de burgerlijke rechten en vrijheden, heeft betrekking op de procedurele waarborgen.[228] Meer bepaald zou artikel 14 onvoldoende procedurele waarborgen bieden aangaande de vrijwaring

[224] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 404.
[225] GILC staat voor Global Internet Liberty Campaign. Het is een vereniging van een 30 tal organisaties die een campagne startten tegen het Cybercrime-Verdrag.
[226] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 405.
[227] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 405.
[228] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 407.

van de rechten van het individu, evenals het recht op een eerlijk proces. Deze kritiek boet toch kracht in, gezien artikel 15 wel waarborgen in die zin voorziet.[229]

141. Samenvattend kan men stellen dat de kritiek die werd geuit op het Cybercrime-Verdrag, niet altijd terecht is. Niettemin is het logisch dat er dergelijke kritiek is gekomen. De waarden die groeperingen ter bescherming van de burgerlijke rechten en vrijheden hoog in het vaandel dragen, stroken niet altijd met de principes die vooropgesteld worden ter bestrijding van cybercriminaliteit. Dat het water tussen beide kampen dan ook diep blijft, en er soms harde kritiek geuit wordt, is dan ook niet onlogisch. Toch is de situatie lang niet zo slechts als sommige groeperingen ons willen doen geloven.

4. HET AANVULLEND PROTOCOL VAN 28 JANUARI 2003

4.1 Algemeen

142. Zoals ik reeds eerder vermeldde kampt het Cybercrime-Verdrag van de Raad van Europa met het gebrek aan bepaling omtrent de bestrijding van racisme en xenofobie. Gezien vrijheid van meningsuiting in Europa een meer stringente invulling krijgt, dan in de Verenigde Staten, gingen laatstgenoemde niet akkoord met de implementatie van een bepaling omtrent het aanzetten tot rassenhaat. Om deze achilleshiel van het Cybercrime-Verdrag te verhelpen, werd er besloten tot het schrijven van een additioneel protocol, gewijd aan deze bepaling. Op deze wijze kon de VS tot het Cybercrime-Verdrag toetreden, en werden er tevens toch stappen genomen tegen racisme en xenofobie. Het protocol kwam tot stand op 28 januari 2003, en kreeg de titel: 'Aanvullend Protocol bij het Cybercrimeverdrag van de Raad van Europa, betreffende de criminalisering van racistische en xenofobische handelingen via computersystemen'.[230]

143. Ondertekening van dit protocol staat enkel open voor staten die eerder al het Cybercrime-Verdrag hebben ondertekend. Tot op heden werd het protocol door 35 staten ondertekend, en door 20 ook effectief geratificeerd. België heeft, net zoals bij het

[229] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 407.
[230] Additional Protocol to the Convention on Cybercrime Council of Europe ETS no. 189, 2003 concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg.

Cybercrime-Verdrag zelf, het protocol ondertekend, maar is nog niet overgegaan tot ratificatie.[231]

4.2 Bespreking van het protocol

4.2.1 Conceptueel kader

144. Het protocol steunt op twee pijlers. Enerzijds, worden een aantal informaticamisdrijven met betrekking tot racisme en xenofobie omschreven, die dienen opgenomen te worden in de nationale wetgeving van de ondertekenende staten. Anderzijds, wordt de verhouding tussen het protocol en het Cybercrime-Verdrag bepaald, met name op welke manier de onderzoeksmachten gedefinieerd in het verdrag van toepassing zijn op racistische en xenofobische misdrijven.[232]

4.2.2 Definiëring

145. Het protocol definieert racistisch en xenofoob materiaal in artikel 2, 1° als volgt: *"any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors."*[233]

4.2.3 Nieuwe incriminaties

146. Het protocol beschrijft enkele nieuwe misdrijven, waarbij van de verdragstaten wordt verwacht dat ze deze inpassen binnen hun nationaal kader. Het betreft hier a-specifieke informaticamisdrijven, waarbij het computersysteem dus enkel de modus aperandi uitmaakt. Op zich is dit logisch, gezien het protocol een aanvulling is van het Cybercrime-Verdrag.[234]

[231] http://conventions.coe.int/Treaty/.
[232] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 398.
[233] Additional Protocol to the Convention on Cybercrime Council of Europe ETS no. 189, 2003 concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg.
[234] H. GRAUX, "Aanvullend protocol bij het Cybercrimeverdrag van de Raad van Europa", *ICRI* 2003, www.internet-observatory.be.

147. De nieuwe incriminaties zijn de volgende:

- *Artikel 3: verspreiding van racistisch en xenofobisch materiaal via een computersysteem*

  Het protocol benadrukt dat elke ondertekenende lidstaat deze inbreuk zou bestraffen. Dit specifieke artikel doelt op verspreiding van dergelijke informatie via websites of nieuwsgroepen. Het sleutelelement van deze bepaling zit hem in het publieke karakter.[235] Paragraaf 2 en 3 van het artikel voorzien in voorbehoudsmogelijkheden voor de ondertekenende staten. Paragraaf 2 betreft de gevallen waarin de discriminerende boodschappen geen verband houden met haat of geweld. Paragraaf 3 gaat nog verder, en laat voorbehoud toe voor het hele artikel indien dit zou indruisen tegen het recht op vrije meningsuiting, zoals dat omschreven wordt in het eigen nationale recht.

- *Artikel 4: bedreigingen uit racistische en xenofobe motieven.*

  Het protocol viseert niet alleen het aanzetten of goedkeuren, maar ook het effectief uiten van racistische of xenofobe dreigementen.[236] Ook hier krijgen de verdragstaten de mogelijkheid tot voorbehoud, zij het iets subtieler. Artikel 4 bepaalt met name dat het dreigement betrekking moet hebben op *"a serious criminal offence as defined under its domestic law"*.[237] Niet alleen krijgen de ondertekenende staten hiermee een ruime appreciatiemarge, het doet tevens afbreuk aan het doel van harmonisatie, gezien de verschillende staten er naar alle waarschijnlijkheid verschillende invullingen zullen op na houden.[238]

- *Artikel 5: beledigingen uit racistische en xenofobe motieven*

  Het aanvullend protocol sanctioneert tevens het uiten van beledigingen in een racistische of xenofobe context. Het dient wel om beledigingen te gaan die op publieke wijze werden geuit. Wederom wordt er een mogelijkheid tot voorbehoud voorzien voor de ondertekenende staten. Voorbehoud kan immers ten aanzien van het hele artikel, evenals een extra voorwaarde voor strafbaarheid in de zin dat de belediging het slachtoffer dient bloot te stellen aan haat, minachting of spot.

---

[235] H. GRAUX, "Aanvullend protocol bij het Cybercrimeverdrag van de Raad van Europa", *ICRI* 2003, www.internet-observatory.be.
[236] H. GRAUX, "Aanvullend protocol bij het Cybercrimeverdrag van de Raad van Europa", *ICRI* 2003, www.internet-observatory.be.
[237] Additional Protocol to the Convention on Cybercrime Council of Europe ETS no. 189, 2003 concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg.
[238] H. GRAUX, "Aanvullend protocol bij het Cybercrimeverdrag van de Raad van Europa", *ICRI* 2003, www.internet-observatory.be.

- *Artikel 6: ontkenning, grove minimalisering, goedkeuring of rechtvaardiging van genocide of misdrijven tegen de menselijkheid.*

  Artikel 6 van het protocol vertoont grote gelijkenissen met het reeds besproken artikel 3. Dit artikel impliceert echter, afwijkend van artikel 3, dat er een ontkenning, minimalisering, goedkeuring of rechtvaardiging dient te zijn. Opnieuw wordt er een recht van voorbehoud voorzien ten aanzien van het hele artikel, of in de vorm van het formuleren van extra voorwaarden.

4.3 Een kritische invalshoek

148. Net als het Cybercrime-Verdrag zelf, is ook het aanvullend protocol niet gespraard gebleven van kritiek. In tegenstelling tot wat het geval was bij het Cybercrime-Verdrag, zien we hier niet echt kritieken als gevolg van een polarisering met groeperingen, maar eerder kritiek op inhoudelijke mankementen.

149. Een eerste kritische noot die zich manifesteert heeft betrekking op de gebruikte definiëring binnen het protocol. Het protocol definieert racistisch en xenofoob materiaal, wat op zich geen probleem stelt. Het opmerkelijke is echter dat er nergens een omschrijving terug te vinden is over wat nu juist onder de term discriminatie wordt verstaan, toch een begrip met een aanzienlijk belang in deze context. Het valt dan ook te betreuren dat het protocol deze interpretatie overlaat aan de ondertekenende staten zelf. Daarenboven gaat het protocol op deze manier voorbij aan haar eigen doel, met name de harmonisering.

150. Een tweede opmerkelijk feit aan de tekst van het aanvullend protocol is het breed uitgesmeerd pallet aan voorbehoudsmogelijkheden dat wordt aangeboden aan de ondertekenende lidstaten. Voor elk van de nieuwe incriminaties voorziet het protocol dergelijke voorbehouds-mogelijkheden. Ongetwijfeld had dit tot doel zoveel mogelijk ondertekenaars aan te trekken, maar niettemin betekent dit toch een sterke beperking van de draagwijdte. Het gevaar bestaat er dan ook in dat het protocol een louter symbolische waarde krijgt.[239]

[239] H. GRAUX, "Aanvullend protocol bij het Cybercrimeverdrag van de Raad van Europa", *ICRI* 2003, www.internet-observatory.be.

Hoofdstuk 6: Aanpak van de Europese Unie

1. OVERZICHT VAN DE GENOMEN INITIATIEVEN

151. Ook de Europese Unie neemt initiatieven in de strijd tegen cybercriminaliteit. Dit is echter niet altijd zo geweest, aanvankelijk stelde de Europese Unie zich namelijk afwachtend op. Zo komen er in de EU-rechtshulpovereenkomst geen bepaling voor die handelen over de strijd tegen cybercriminaliteit. De Groep Wederzijdse Rechtshulp in Strafzaken (GWRS) heeft zich nooit in deze materie verdiept.[240] In april 1997 zette de EU zijn eerste stappen in de vorm van een actieplan, aangenomen door de Groep op Hoog Niveau (GHN), ter bestrijding van de georganiseerde criminaliteit. Dit actieplan benadrukte het belang om actie te ondernemen tegen high-tech criminaliteit.[241] Een volgende stap volgde op 25 januari 1999, wanneer een Communautair Actieplan ter bevordering van het veilige gebruik van Internet werd uitgevaardigd.[242]

152. Op 27 november 2001 vond in Brussel, op initiatief van de Europese Commissie, het 'EU Forum on Cybercrime' plaats.[243] Het onderwerp bij uitstek tijdens deze conferentie was de bewaring van gegevens van internetverkeer.[244] Op 19 april 2002 stelde de Europese Commissie een voorstel voor, genaamd 'proposal for a Council framework decision on attacks against information systems'.[245] [246] Het voorstel werd in 2005 door de Raad aangenomen, en omgedoopt tot het Kaderbesluit 2005/222/JBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen.[247] Aan het Kaderbesluit 2005/222/JBZ is, gezien het aanzienlijk belang van het document, een aparte titel gewijd. Het kaderbesluit zal besproken worden in het laatste punt van dit hoofdstuk.

---

[240] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 412.
[241] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 413.
[242] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 413.
[243] Discussion Paper for Expert's Meeting on Retention of Traffic Data, 6 november 2001, http://ec.europa.eu.
[244] EU forum on Cybercrime Plenary session, 27 November 2001, Brussels, http://ec.europa.eu..
[245] Commission proposal for a Council framework decision on attacks against information systems, 19 april 2002, http://ec.europa.eu.
[246] Commission proposal for a Council framework decision on attacks against information systems, 19 april 2002, http://ec.europa.eu.
[247] Kaderbesluit Raad van Europa 2005/222/JBZ, 24 februari 2005 over aanvallen op informaticasystemen, *PB*, 16 maart 2005, Nr. L 69/67.

153. In november 2007 werd door de Europese Commissie een 'expert meeting on cybercrime' georganiseerd.[248] Deze conferentie betekende een volgende stap in het beleid van de Europese Unie aangaande cybercriminaliteit, zoals het werd uitgelijnd door de Europese Commissie. Exact een jaar later, in november 2008, stelde de Europese Raad een strategie[249] voor om de strijd tegen cybercriminaliteit op te drijven: *"The European Commission has cooperated closely with the French Presidency and the Member States in the elaboration of a series of practical measures to fight cybercrime. The new strategy recommends reinforcing partnership between the police and the private sector by better knowledge-sharing on investigation methods and trends in cybercrime. It also encourages both parties to respond quickly to information requests, resort to remote searches, cyber patrols for online tracking of criminals and joint investigations across borders. The strategy also calls for the setting up an alert platform in the short term, where reports on crime committed on the Internet, such as posting of illegal content, in EU would be pooled for cross-checking by Europol."* [250]

154. Op 30 maart 2009 stuurde de Europese Commissie een mededeling de wereld in aangaande de bescherming van kritieke informatie-infrastructuur, getiteld: 'Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht'.[251] Het doel was om de ongelijke en ongecoördineerde nationale benaderingen enigszins op mekaar af te stemmen, en op die manier internationale samenwerking te bewerkstelligen. Men wou dus gaan naar meer EU-coördinatie en -samenwerking. Er werden in dit kader 5 pijlers als basis vooropgesteld, om deze uitdagingen aan te gaan. Deze 5 pijlers zijn de volgende: [252]

- *paraatheid en preventie: paraatheid op alle niveaus verzekeren;*
- *detectie en respons: voorzien in mechanismen voor vroegtijdige waarschuwing;*
- *mitigatie en herstel: versterken van EU-verdedigingsmechanismen voor Kritieke Informatie Infrastructuren;*
- *internationale samenwerking: internationaal bevorderen van EU-prioriteiten;*

[248] www.cybercrimelaw.net/documents/cybercrime_history.pdf.
[249] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827.
[250] P. MURPHY, "Remote search and the invisible elephant", *ZDNet* 28 januari 2009, www.zdnet.com.
[251] Mededeling Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende de bescherming van kritieke informatie-infrastructuur, 30 maart 2009, Brussel.
[252] Mededeling Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende de bescherming van kritieke informatie-infrastructuur, 30 maart 2009, Brussel.

- *criteria voor de ICT-sector: ondersteunen van de tenuitvoerlegging van de Richtlijn inzake de identificatie van en aanmerking als Europese kritieke infrastructuren.*

155. Op 20 november 2010 vond er in Lissabon een EU-VS top plaats. Tijdens deze bijeenkomst werd er besloten tot de oprichting van een EU-VS werkgroep aangaande internetveiligheid en internetcriminaliteit. Deze top kende zijn vervolg in Washington DC, op 28 november 2011. Net voor de top, op 3 november 2010, werd er voor het eerst een oefening, met betrekking tot de internetveiligheid, gehouden.[253] Deze oefening ging als de 'Cyber Atlantic 2011' door het leven, en was een initiatief van de EU en de VS, ondersteund door Enisa[254] en het US Department of Homeland Security. De hele dag lang werden er simulaties gehouden van cyber-aanvallen, om zo te achterhalen of de EU en de VS hierop passend reageerden. Na de top in Washington legden de leiders van de twee grootmachten volgende verklaring af: *"We welcome the progress made by the EU-U.S. Working Group on Cyber security and Cybercrime, notably the successful Cyber Atlantic 2011 exercise. We endorse its ambitious goals for 2012, including combating online sexual abuse of children; enhancing the security of domain names and Internet addresses; promotion of international ratification, including by all EU Member States, of the Budapest Convention on Cybercrime ideally by years end; establishing appropriate information exchange mechanisms to jointly engage with the private sector; and confronting the unfair market access barriers that European and U.S. technology companies face abroad."*[255]

156. Op 28 maart 2012 werd bekend dat de Europese Commissie wou overgaan tot de oprichting van een 'European Cybercrime Centre' in Den Haag. Cecilia Malmström, Europees Commissaris voor Binnenlandse Zaken, stelde het centrum voor.[256]Eind 2001 zag een soortgelijk initiatief al eens het levenslicht. Spanje, de toenmalige voorzitter van de EU, pleitte destijds voor een waarnemingscentrum voor high-tech criminaliteit.[257] [258] Dit centrum zou opgenomen worden binnen Europol. Het doel van dit centrum was om vroegtijdig

[253] www.enisa.europa.eu.
[254] Enisa staat voor European Network and Information Security Agency. De instelling helpt de Europese Commissie en de lidstaten van de EU om te gaan met informatica-veiligheidsproblemen en hoe deze te vermijden.
[255] www.whitehouse.gov/the-press-office/2011/11/28/joint-statement-us-eu-summit.
[256] S. GEUKENS, "Eu-Commissie start centrum tegen cybercrime", De Morgen 28 maart 2012, www.demorgen.be.
[257] www.security.nl/artikel/2883/1/Europol_krijgt_waarnemingscentrum_voor_hightechcriminaliteit.html.
[258] Nota Raad 15456/01, betreffende het voorstel van het Spaanse voorzitterschap en initiatief van Europol tot instelling bij Europol van een waarnemingscentrum voor computercriminaliteit, 18 december 2001, 5.

bedreigingen op te sporen, evenals een strategie ontwikkelen voor de bescherming van vitale informaticastructuur. Het centrum diende tevens de rol van alarmcentrale op zich te nemen, daar er in Europa op dat moment nog geen centraal punt bestond waar bedrijven en overheden zich tot konden wenden. Het waarnemingscentrum zou een totaalpakket uitmaken, dat het hele spectrum van de high-tech criminaliteit moest bestrijken. Het voorstel werd destijds maar met een lauw enthousiasme onthaalt. De tegenkanting kwam uit verschillende hoeken. Een aantal lidstaten had een niet zo hoge dunk over het hele concept, maar de zwaarste tegenwind ondervond Spanje vanuit de hoek van de Europese Commissie.[259] Algemeen werd ervan uitgegaan dat de Europese Commissie angst had dat Europol een iets te grote rol zou spelen op dit terrein, waardoor de Commissie een deel van haar macht zag verdwijnen. Het waarnemingscentrum voor high-tech criminaliteit was een kort leven beschoren, het dossier werd in de koelkast gestoken. Onlangs zag het hele idee echter opnieuw het levenslicht, in de vorm van het European Cybercrime Centre. De krachtlijnen mogen dan wel op bepaalde punten licht verschillen, de gelijkenissen zijn in ieder geval treffend.

157. Het Cybercrime Centre, dat gehuisvest zal worden bij Interpol, zou operationeel moeten zijn begin 2013 en zal de basis worden van de Europese strijd tegen cybercriminaliteit.[260] Het belang van dit centrum wordt verwoord door Rob Wainwright, directeur van Interpol: *"The establishment of the European Cybercrime Centre will be a landmark development in the EU's fight against cybercrime. I am delighted that the Commission has proposed its establishment at Europol. Organized crime groups, terrorist groups and other criminals are quick to exploit the opportunities afforded by developments in technology, and the time is ripe for the authorities to get one step ahead. The European Cybercrime Centre will provide governments, businesses and citizens throughout the Union with the tools to tackle cybercrime. Building on Europol's proven track record and unique expertise in this area, and with the support of the Member States, other EU bodies, international partners, and the private sector, the European Cybercrime Centre will make the EU smarter, faster and stronger in its fight against cybercrime."* [261]

[259] www.security.nl/artikel/2883/1/Europol_krijgt_waarnemingscentrum_voor_hightechcriminaliteit.html.
[260] X., "Den Haag krijgt Europees cybercrimecentrum", *De Stentor* 28 maart 2012, www.destentor.nl.
[261] www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417.

2. HET KADERBESLUIT 2005/222/JBZ VAN DE EUROPESE RAAD

2.1 Algemeen

158. Het Kaderbesluit 2005/222/JBZ van de Europese Raad over aanvallen op informatiesystemen [262] dient gesitueerd te worden binnen het kader van het eEurope-actieplan.[263] Het preciseert in zekere zin het Cybercrime-Verdrag van de Raad van Europa.

159. Het kaderbesluit heeft als doelstelling de samenwerking tussen de justitiële en andere bevoegde instanties van de lidstaten te bevorderen door middel van harmonisatie van de strafrechtelijke bepalingen. Verder heeft het kaderbesluit eveneens het doel de verschillende activiteiten op internationaal niveau, zoals de activiteiten in de schoot van de G8 en de Raad van Europa, verder te ontwikkelen.[264]

160. Het kaderbesluit trad in werking op 16 maart 2005. De lidstaten hadden tot 16 maart 2007 de tijd om de nodige maatregelen te treffen om te voldoen aan de bepalingen van het kaderbesluit.

2.2 Summiere artikelsgewijze bespreking

161. Artikel 1 van het kaderbesluit is gewijd aan de definities. Deze lopen in grote lijnen gelijk met de definities die terug te vinden zijn in het Cybercrime-Verdrag, al zijn ze hier meer gespecifieerd. De essentie blijft echter dezelfde.

162. De artikelen 2, 3 en 4 bespreken de incriminaties. Net als in het Cybercrime-Verdrag is er voorzien in de strafbaarstelling van volgende misdrijven: [265]

- onrechtmatige toegang tot informatiesystemen;
- onrechtmatige systeemverstoring;
- onrechtmatige gegevensverstoring.

[262] Kaderbesluit Raad van Europa 2005/222/JBZ, 24 februari 2005 over aanvallen op informaticasystemen, *PB*, 16 maart 2005, Nr. L 69/67.
[263] Kaderbesluit Raad van Europa 2005/222/JBZ, 24 februari 2005 over aanvallen op informaticasystemen, *PB*, 16 maart 2005, Nr. L 69/67.
[264] Kaderbesluit Raad van Europa 2005/222/JBZ, 24 februari 2005 over aanvallen op informaticasystemen, *PB*, 16 maart 2005, Nr. L 69/67.
[265] http://eur-lex.europa.eu/.

163. Artikel 5 vermeldt tevens dat op de ondertekenende staten de verplichting rust de uitlokking, medeplichtigheid en de poging tot bovenstaande incriminaties strafbaar te stellen. Deze bepaling is vergelijkbaar met artikel 11 van het Cybercrime-Verdrag.

164. De artikelen 6 en 7 vormen ook een innovatie ten opzichte van het Cybercrime-Verdrag, in die zin dat ze bepalen wat de minimale maximumstraf is die opgelegd moet worden indien de cybercriminaliteit werd gepleegd in het kader van een criminele organisatie.[266]

165. De artikelen 8 en 9 van het kaderbesluit behandelen de aansprakelijkheid van rechtspersonen. Beide bepalingen zijn veel uitgebreider dan het soortgelijke artikel in het Cybercrime-Verdrag, met name artikel 12. Het kaderbesluit bespreekt eveneens de bestraffing van de rechtspersonen, en dat op een meer concrete manier dan in het verdrag.[267]

166. Verder bevat het kaderbesluit nog bepalingen omtrent de rechtsmacht en de uitwisseling van informatie, bepalingen die vergelijkbaar zijn met deze uit het Cybercrime-Verdrag.

167. Het grootste verschil tussen het Cybercrime-Verdrag en het kaderbesluit zit hem in het feit dat het laatstgenoemde nergens gewag maakt van inhoudsgerelateerde misdrijven.[268] Dit is echter niet problematisch, gezien deze categorie misdrijven al behandeld werd in het Cybercrime-Verdrag zelf, evenals in het aanvullend protocol.

2.3 Richtlijn tot intrekking van Kaderbesluit 2005/222/JBZ

168. Op 30 september 2010 kondigden Eurocommissarissen Cecelia Malmström en Neelie Kroes nieuwe maatregelen aan in de strijd tegen cybercrime.[269] [270] Het betreft twee nieuwe maatregelen. Vooreerst betreft het een voorstel voor een richtlijn over de aanpak van nieuwe vormen van computercriminaliteit, zoals grootschalige cyberaanvallen. De tweede maatregel bestaat uit een voorstel voor een verordening ter versterking en modernisering van het

[266] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (433) 453.
[267] Kaderbesluit Raad van Europa 2005/222/JBZ, 24 februari 2005 over aanvallen op informaticasystemen, *PB*, 16 maart 2005, Nr. L 69/67.
[268] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (433) 453.
[269] http://europa.eu.
[270] http://oerlemansblog.weblog.leidenuniv.nl/2010/11/05/nieuw-voorstel-voor-een-europese-richtli.

Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA).[271] Ik zal hier de nadruk leggen op het eerste voorstel.

169. In de schoot van de Europese Commissie ontstond een voorstel voor een richtlijn van het Europese Parlement en de Raad over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ van de Raad.[272] Het idee voor een nieuwe richtlijn kwam er na een verslag van de Europese Commissie[273] over de tenuitvoerlegging van het kaderbesluit. De algemene teneur was positief, de meeste lidstaten hadden progressie geboekt wat betreft de uitvoering van het kaderbesluit. Niettemin deze positieve noot wees de Commissie op het volgende: *"Sinds het vaststellen van het kaderbesluit hebben recente aanvallen in heel Europa allerlei nieuwe bedreigingen aan het licht gebracht, met name het zich voordoen van omvangrijke gelijktijdige aanvallen op informatiesystemen en een toenemend crimineel gebruik van zo gehete botnets"*.[274] De Europese Commissie was de mening toegedaan dat het bestaande Kaderbesluit 2005/222/JBZ op dit punt tekort schoot, en achtte de tijd rijp voor een nieuw document. Het voorstel tot richtlijn is een reactie op de "*groeiende bedreiging en de bezorgdheid over mogelijke terroristische of politiek gemotiveerde aanvallen op informatiesystemen die deel uitmaken van de vitale infrastructuur van de lidstaten en de Unie".*[275] Het voorstel is dan ook in eerste instantie gericht op de problematiek van de specifieke informaticacriminaliteit, waaronder de hierboven genoemde botnets[276] vallen.

170. Het gebruik van de term 'intrekking' met betrekking tot het Kaderbesluit 2005/222/JBZ is enigszins sterk uitgedrukt. De bestaande bepalingen worden immers overgenomen, aangevuld met nieuwe elementen.[277] Het voorstel tot richtlijn voert enkele nieuwe elementen in, de moeite waard om van nader bij te bekijken. Zo stelt de richtlijn in artikel 6 onrechtmatige onderschepping strafbaar. In artikel 7 wordt de productie, verkoop, aanschaf voor gebruik, invoer, verspreiding of het op andere wijze beschikbaar maken van

[271] http://europa.eu/.
[272] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:NL:PDF.
[273] Verslag van de Commissie aan de Raad op basis van artikel 12 van het kaderbesluit van de Raad van 24 februari 2005 over aanvallen op informatiesystemen, COM(2008), 448.
[274] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:NL:PDF.
[275] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:NL:PDF.
[276] Een botnet is een groep van computers die besmet zijn met malware (kwaadaardige software). Via deze malware kan een phisher de controle uitoefenen over verschillende computers en kan hij verborgen blijven op het Internet omdat hij opereert via de computers van andere mensen.
[277] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:NL:PDF.

computerprogramma's of computerwachtwoorden voor het plegen van de vernoemde feiten strafbaar gesteld.

171. Misschien wel de meest ingrijpende veranderingen vallen vast te stellen in artikel 9 en 10 van de richtlijn, welke betrekking hebben op de sancties en de verzwarende omstandigheden. In vergelijking met het kaderbesluit stijgt de strafmaat in deze richtlijn meer dan aanzienlijk. Artikel 14 van de richtlijn versterkt daarenboven het concept van de operationele meldpunten, door de verplichting op te leggen dat er op dringende verzoeken binnen de 8 uur moet gereageerd worden. Een laatste vernieuwing vinden we in artikel 15 van de richtlijn. Dit artikel verplicht de lidstaten tot het creëren van een systeem voor het registeren, aanmaken en verstrekken van statistische gegevens over de in de richtlijn beschreven strafbare feiten. Deze gegevens worden dan, door elk van de lidstaten, overgemaakt aan de Europese Commissie. Op deze manier probeert de Europese Commissie onmiskenbaar meer zicht te krijgen over de situatie. De overige, hier niet besproken, artikels zijn identiek aan die uit het Kaderbesluit 2005/222/JBZ.

Hoofdstuk 7: Conclusie

172. Eens te meer blijkt het dat cybercriminaliteit de meningen niet onberoerd laat. Vele grote internationale organisaties hebben zich al over de problematiek gebogen.

173. Ondanks dat cybercriminaliteit geen absolute prioriteit is voor een organisatie als de OESO, was ze wel de eerste met richtlijnen omtrent cybercrime. De organisatie heeft in dit kader al tal van rapporten vrijgegeven omtrent het onderwerp.

174. De Verenigde Naties spelen ook een belangrijke rol in dit kader. Spijtig genoeg brengt de VN weinig concrete oplossingen aan de dag. Het blijft eerder bij veel goede bedoelingen, echte regelgeving is er nog niet ontstaan. Toch is de VN één keer heel dicht geweest bij een nieuwe, concrete tekst. In 2010 lag er immers een ontwerp voor een nieuwe basistekst, in de strijd tegen cybercriminaliteit, op tafel. Door onderlinge discussies tussen de verschillende lidstaten is het echter nooit zover gekomen.

175. Ook de G8 houdt de ontwikkelingen omtrent cybercriminaliteit nauwlettend in het oog. Het blijft dan vooral beperkt tot rapporten en verklaringen bij de G8-toppen. Vermits de G8 geen groot ledenbestand heeft, blijft de uitwerking vaak enigszins beperkt. Dit valt te betreuren, want de initiatieven van de G8 zijn best lovenswaardig te noemen.

176. De Raad van Europa trekt in dit kader, met het Cybercrime-Verdrag, alle aandacht naar zich. Dat verdrag was het eerste, en tot op vandaag, het enige internationale verdrag gericht op de aanpak van cybercriminaliteit. Het belang van dit verdrag kan niet genoeg benadrukt worden. Het zette de krijtlijnen uit wat strafbaarstellingen en bepalingen van strafprocesrecht betreft, en zorgde voor een tendens van uniformisering. Het blijft echter een spijtige zaak dat de VS het verdrag pas heeft ondertekend, nadat de bepalingen omtrent racisme en xenofobie, naar een aanvullend protocol werden verbannen.

177. Ook de EU heeft een belangrijke rol gespeelt in het kader van de strijd tegen cybercriminaliteit. De EU is echter later van start gegaan dan de rest van deze instellingen, vermoedelijk omdat men overlappingen met de initiatieven van de Raad van Europa wou vermijden. Het Kaderbesluit 2005/222/JBZ is een zeer belangrijk document geworden, waarbij de EU haar strategie kenbaar heeft gemaakt.

DEEL V: De Belgische aanpak inzake cybercriminaliteit

Hoofdstuk 1: Inleiding

178. In dit deel zal de Belgische aanpak van cybercriminaliteit worden behandeld. Centraal staat de wet van 28 november 2001 inzake informaticacriminaliteit, hierna WIC, evenals welke invloed deze wet heeft op de opsporing en vervolging van cybercriminaliteit in ons land.

Hoofdstuk 2: De wet van 28 november 2000 inzake informatica-criminaliteit

1. DE STAND VAN ZAKEN VOORAFGAAND AAN DE WET

179. In de jaren voorafgaand aan de totstandkoming van de wet van 28 november 2000 inzake informaticacriminaliteit beschikte België niet over specifieke wetgeving betreffende de bestraffing van informaticamisdrijven. Dit had tot gevolg dat de rechter vaak zijn toevlucht moest zoeken tot artikelen die initieel, in geen enkel opzicht, de bestraffing van zulke feiten voor ogen hadden.[278] Het bestraffen van cybercrimemisdrijven aan de hand van strafbepalingen die daar terminologisch niet voor geschikt zijn, was niet houdbaar. Dit bleek eens te meer uit de hieruit voortvloeiende rechtspraak, die in bepaalde gevallen kant noch wal raakte.[279] In dat opzicht kende België twee geruchtmakende zaken, die duidelijk hebben gemaakt dat de Belgische wetgeving met een lacune kampte. Het betreft de *'Bistel'*-zaak en de zaak *'ReDaTtacK'*.

180. De *'Bistel'*-zaak was belangrijk in die zin dat het de eerste keer was in België dat de inbraak in een computersysteem strafbaar werd gesteld.[280] Op het feitenrelaas en de uitspraken van de correctionele rechtbank en het hof van beroep zal hier niet dieper worden ingegaan, gezien dit reeds eerder werd besproken.[281] De tweede zaak handelt over Frans Devaere, die onder zijn alias 'ReDaTtacK' enkele sites hackte. Meer bepaald kraakte hij meerdere Skynet- en Generale Bank-bestanden, door middel van de login-gegevens van een

[278] H. GRAUX, "Wet inzake informaticacriminaliteit.", *ICRI* 2001, http://www.internet-observatory.be.
[279] Zo werd in de Bistel-zaak gepoogd computerinbraak als diefstal van computerenergie te kwalificeren.
[280] B. DE SCHUTTER, "Het Belgische Bistel-syndroom", *Computerr.* 1991, (164) 166.
[281] Voor het uitgebreide relaas zie randnummer 30 e.v..

klant, die hiervoor geen toestemming had gegeven. Hij had eveneens bij de Generale Bank kennis genomen van een aantal bancaire transacties. Vervolgens stuurde hij deze gegevens naar een dertigtal bestemmelingen in de pers, gevolgd door de mededeling dat hij de betrokken gegevens nadien had vernietigd. Frans Devaere diende voor de correctionele rechtbank te verschijnen, die hem veroordeelde op grond van artikel 109ter D lid 1, 3° en 4° van de Telecomwet, wegens de schending van het telecommunicatiegeheim.[282] Voor de hacking van de Generale Bank werd hij echter vrijgesproken. Dit omwille van het feit dat hij enkel online bewerkingen kon zien, maar geen saldi en dergelijke meer. De rechter oordeelde dan ook dat dit geen gegevens inzake telecommunicatie zijn, waardoor hij wat dit betreft niet kon worden veroordeeld op grond van de Telecomwet.[283]

181. Deze twee zaken illustreerden de dringende noodzaak aan wetgevende initiatieven betreffende de aanpak van informaticacriminaliteit.

2. TOTSTANDKOMING VAN DE WET VAN 28 NOVEMBER 2000 INZAKE INFORMATICACRIMINALITEIT

182. Het ontstaan van de wet van 28 november 2000 heeft heel wat voeten in de aarde gehad. Reeds in 1983 kreeg Bart De Schutter, professor aan de VUB, van de OESO de opdracht om via een studie na te gaan in welke mate het Belgische strafrecht diende te worden aangepast aan het fenomeen van informaticacriminaliteit.[284] De studie nam enkele jaren in beslag, waarna Bart De Schutter in 1987 zijn rapport indiende. Het hierop volgende decennium werd het opnieuw windstil. Pas begin 1999 werden de eerste stappen gezet, toen voormalig minister van Justitie Tony Van Parys een voorontwerp van wet indiende in de Kamer. Op het einde van datzelfde jaar, in november, werd het voorontwerp weer opgevist en opnieuw ingediend. Ditmaal door Rik Daems, Marc Verwilghen en Rudy Demotte. Het ontwerp werd in maart 2000 door de Kamer goedgekeurd, maar de senaat liet het ontwerp evoceren en amenderen.[285] Na veel touwgetrek tussen de Kamer en de Senaat werd het ontwerp op 26 oktober 2000 in

[282] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 437.
[283] R. DE CORTE , "ReDaTtacK krijgt deksel op de neus", *Juristenkrant* 2001, 5.
[284] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 421.
[285] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 422.

haar oorspronkelijke versie goedgekeurd.[286] Met deze goedkeuring beschikte België vanaf dat moment weer over adequate wetgeving, aangepast aan het nieuwe fenomeen van informaticacriminaliteit.[287] De wet werd op 3 februari 2001 gepubliceerd in het Belgisch staatsblad, en trad 10 dagen later in werking.

3. BESPREKING VAN DE WET VAN 28 NOVEMBER 2000 INZAKE INFORMATICA-CRIMINALITEIT

183. België heeft zich met de wet van 28 november 2000, willen wapenen tegen cybercriminaliteit. De wettekst sluit grotendeels aan bij de meeste Europese landen. Er worden op drie niveaus nieuwigheden ingevoerd:[288]

- Vooreerst worden er enkele nieuwe strafbaarstellingen in het Strafwetboek ingevoerd:
  - valsheid in informatica;
  - informaticabedrog;
  - ongeoorloofde toegang;
  - informaticasabotage.
- Vervolgens worden er ook op het gebied van het strafprocesrecht nieuwigheden ingevoerd. Zo krijgen gerechtelijke onderzoekers volgende bevoegdheden:
  - databeslag;
  - netwerkzoeking;
  - medewerkingsplicht;
  - aanvullingen van de artikelen 90ter, 90quater en 90septies Sv.
- Tenslotte wordt er tevens voorzien in een aanvulling van de Belgacomwet, in die zin dat er nieuwe verplichtingen worden opgelegd aan operatoren van telecommunicatienetwerken, en verstrekkers van telecommunicatiediensten.

[286] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 422.
[287] M. TAEYMANS, "De wet informaticacriminaliteit in werking getreden", *Computerr.* 2001, (103) 103.
[288] S. EVRARD, "La loi du 28 novembre 2000 relative à la criminalité informatique, *J.T.* 2001 (241) 243.

3.1 Bepalingen tot aanvulling van het Strafwetboek

3.1.1 Valsheid in informatica (artikel 201bis Sw.)

184. Deze strafbaarstelling, voorzien in artikel 4 WIC, kan beschouwd worden als de online variant van de klassieke bepaling omtrent de valsheid in geschriften. Deze bepaling werd ingevoerd om een einde te stellen aan de discussie of valsheid in geschrifte als bepaling kan worden toegepast in een informaticacontext.[289] Het artikel beoogt de opzettelijke vervalsing via datamanipulatie met betrekking tot juridisch relevante gegevens, te bestraffen.[290] Het betreft dan meer bepaald de gevallen waarin kredietkaarten, digitale handtekeningen en andere interessante documenten worden nagemaakt of vervalst. Valsheid in informatica heeft betrekking op het wijzigen, wissen of veranderen van de aanwending van gegevens in een informaticasysteem, zodat de juridische draagwijdte van deze gegevens verandert. Opmerkelijk is wel dat hier, in tegenstelling tot bij de klassieke valsheid in geschrifte, geen bijzonder opzet vereist is. Het feit dat men wetens en willens de materieel omschreven verrichting begaat, volstaat als dusdanig.[291]

185. Het plegen van valsheid in informatica wordt gestraft met een gevangenisstraf van zes maanden tot vijf jaar, en/of met een geldboete van zesentwintig euro tot honderdduizend euro. Pogingen tot valsheid in informatica worden eveneens strafbaar gesteld, met name met een gevangenisstraf van zes maanden tot drie jaar en met een geldboete van zesentwintig euro tot vijftigduizend euro, of met een van die straffen alleen. Verder poogt de wet recidivisten af te schrikken, voor hen wordt voorzien in een stringent regime.

3.1.2 Informaticabedrog (artikel 504quater Sw.)

186. De tweede nieuwe strafbaarstelling die de WIC invoert, in artikel 5, betreft informaticabedrog. Deze incriminatie heeft tot doel de personen te bestraffen die een onrechtmatig vermogensvoordeel verwerven door middel van datamanipulatie. De term ‘onrechtmatig vermogensvoordeel’ is het sleutelbegrip binnen deze bepaling. Zonder dit aspect is er geen sprake van informaticabedrog. Verder vereist informaticabedrog tevens dat

[289] H. GRAUX, “Wet inzake informaticacriminaliteit.”, *ICRI* 2001, http://www.internet-observatory.be.
[290] S. VANSTEENHUYSE en P. T’JONCK, “Cybercriminaliteit en privacy”, in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 434.
[291] H. GRAUX, “Wet inzake informaticacriminaliteit.”, *ICRI* 2001, http://www.internet-observatory.be.

men handelt met een bedrieglijk opzet, of met de bedoeling te schaden. Wanneer, bijvoorbeeld, een student inbreekt in het informaticasysteem van zijn universiteit om zijn examenresultaat te wijzigen, maakt dit geen informaticabedrog uit, gezien er geen vermogensvoordeel is.[292] Dit in de veronderstelling dat het diploma niet als een dusdanig vermogensvoordeel wordt beschouwd door de rechtspraak.[293] Informaticabedrog is, net zoals de valsheid in informatica een computergerelateerde variant is van de klassieke valsheid in geschrifte, een gemoderniseerde versie van de klassieke figuur van de oplichting.[294]

187. Een goed voorbeeld van wat men onder informaticabedrog dient te verstaan kan men vinden in de *'Orange'*-zaak. Begin 2001 kwam er een grootschalige fraude met zogenaamde 'pre-pay'-kaarten van Orange aan het licht. Indien men over een dergelijke kaart beschikte, kon men via het invoeren van een speciale code gratis bellen. Deze code werd langs allerlei kanalen verspreid. Het bedrijf Orange liep hierdoor een miljoenenverlies op. Als men in dit kader artikel 504quater van de Strafwet zou toepassen, dan kan zowel diegene die de code gebruikte, doorzond of trachtte in te voeren gestraft worden. [295]

188. Informaticabedrog wordt bestraft met een gevangenisstraf van zes maanden tot vijf jaar en met een geldboete van zesentwintig euro tot honderdduizend euro, of met een van die straffen alleen. Poging tot het plegen van het misdrijf wordt gestraft met een gevangenisstraf van zes maanden tot drie jaar en met een geldboete van zesentwintig euro tot vijftigduizend euro, of met een van die straffen alleen. Voor recidivisten wordt er, net zoals bij de valsheid in informatica, voorzien in een verzwaard regime.

3.1.3 Ongeoorloofde toegang (artikel 550bis Sw.)

189. In artikel zes van de WIC wordt de ongeoorloofde toegang, ook wel hacking genoemd, strafbaar gesteld. Meer bepaald gaat het om misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen. Concreet wordt er een onderscheid gemaakt

[292] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 435.
[293] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, 435.
[294] H. GRAUX, "Wet inzake informaticacriminaliteit.", *ICRI* 2001, http://www.internet-observatory.be.
[295] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 435.

tussen interne en externe hacking.[296] Interne hacking betreft het geval waarin iemand, die wel een toegangsbevoegdheid heeft, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt. Voor interne hacking is een bijzonder opzet vereist, dit in tegenstelling tot externe hacking, waarvoor een algemeen opzet volstaat. Externe hacking betreft de situatie waarin een persoon, die op de hoogte is van het feit dat hij niet gerechtigd is, zich toegang verschaft tot een informaticasysteem, of zich daarin handhaaft.

190. De bestraffing verschilt voor beide soorten hacking. Hij die zich schuldig maakt aan externe hacking, wordt gestraft met een gevangenisstraf van drie maanden tot een jaar en met een geldboete van zesentwintig euro tot vijfentwintig duizend euro, of met een van die straffen alleen. Diegene die zich schuldig maakt aan interne hacking, wordt dan weer gestraft met een gevangenisstraf van zes maanden tot twee jaar en met geldboete van zesentwintig euro tot vijfentwintigduizend euro, of met een van die straffen alleen. Opmerkelijk hierbij is dat de wetgever de straf voor externe hacking op hetzelfde niveau brengt als voor interne hacking, indien de externe hacking met bedrieglijk opzet gebeurt. In de meeste gevallen zal dit wel degelijk het geval zijn, waardoor interne en externe hacking qua ernst gelijkgeschakeld worden.

191. Het artikel voorziet tevens in verzwarende omstandigheden, zoals bedrijfsspionage, tijdsdiefstal en het beschadigen van computers. Aan deze feiten worden dan ook verhoogde straffen gekoppeld. Poging tot, evenals recidivisme, wordt net als bij de twee voorgaande incriminaties strafbaar gesteld. Ook heling valt onder het toepassingsgebied van dit artikel. Op deze wijze wou men de handel in paswoorden en dergelijk meer beperken, dit terwijl heling traditioneel enkel van toepassing was op materiële goederen. Ook voorbereidingshandelingen zijn strafbaar gesteld, waarmee men doelt op zogenaamde hackertools.[297]

192. Misschien wel het meest opvallende aan dit artikel is dat de opdrachtgever zwaarder wordt gestraft als de eigenlijke dader zelf.[298] Achter deze, op het eerste zich ietwat vreemde vaststelling, zit een logische verklaring. Professionele criminelen schakelen immers vaak

[296] H. GRAUX, "Wet inzake informaticacriminaliteit.", *ICRI* 2001, http://www.internet-observatory.be.
[297] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 424.
[298] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 438.

computerfreaks in om hen te helpen bij hun daden, gezien zij zelf weinig technisch onderlegd zijn. Door de opdrachtgever zwaarder te straffen kan men zich enigszins richten op de grote vissen, in plaats van de loopjongen van dienst.

3.1.4 Informaticasabotage (artikel 550ter Sw.)

193. De wet van 28 november 2000 voert tevens artikel 550ter in. Dit artikel is gericht tegen informaticasabotage. Concreet dient het te gaan om een persoon die, met het oogmerk om te schaden gegevens in een informaticasysteem invoert, wijzigt, wist of met enig ander technologisch middel de aanwending van gegevens in een informaticasysteem verandert. Het typevoorbeeld dat deze incriminatie voor ogen heeft, is het geval waarin virussen of worms in een systeem worden ingebracht, waardoor het systeem onbruikbaar wordt.[299]

194. Informaticasabotage wordt bestraft met een gevangenisstraf van zes maanden tot drie jaar en met een geldboete van zesentwintig euro tot vijfentwintigduizend euro, of met één van die straffen alleen. Wanneer het misdrijf gepleegd wordt met bedrieglijk opzet of met het oogmerk om te schaden, bedraagt de gevangenisstraf zes maanden tot vijf jaar. Artikel 550ter Sw. maakt een onderscheid tussen schade die toegebracht wordt aan data, en schade die wordt toegebracht aan het systeem zelf. Deze laatste variant wordt zwaarder bestraft, gezien de grotere impact.[300] Voorbereidende handelingen zijn, net zoals bij de ongeoorloofde toegang, strafbaar gesteld. De poging tot het plegen van dit misdrijf is, opmerkelijk genoeg, niet strafbaar gesteld. Dit omwille van het feit dat de bewijslast dienaangaande niet voor de hand liggend is. Recividisme is daarentegen wel strafbaar gesteld.

3.1.5 Conclusie

195. De Belgische wetgever heeft er, met de invoering van deze nieuwe strafbaarstellingen, voor gezorgd dat België zich kan wapenen tegen cybercriminaliteit. Met betrekking tot de nieuwe incriminaties kunnen er enkele vaststellingen gedaan worden, de moeite waard om van nader bij te bekijken.

---

[299] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 424.
[300] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 439.

196. Vooreerst valt op dat niet alleen het effectief plegen van het misdrijf, maar eveneens de poging tot, strafbaar wordt gesteld. Dit geldt voor alle nieuwe incriminaties, behalve informaticasabotage, gezien de poging in dit laatste geval zeer moeilijk te bewijzen valt. Ook het recidivisme wordt hard aangepakt, gezien er wordt voorzien in een verdubbeling van de straffen. Het feit dat zowel het plegen, de poging tot en de herhaling streng wordt bestraft, is naar mijn mening een goede zaak. De wetgever heeft mijns inziens ook een klare kijk gehanteerd door in het geval van ongeoorloofde toegang, de opdrachtgever zwaarder te straffen dan de dader zelf. De wetgever wil op deze manier de wortels van de problematiek aanpakken, in plaats van zich te focussen op de uiterlijke verschijningsvorm. Dit kan alleen maar beschouwd worden als zijnde een goede zaak.

197. Vervolgens valt ook op dat de wetgever zich niet heeft laten verleiden tot het formuleren van allerlei technische definities. Dat dit een goede zaak is, behoeft geen betoog. Op deze wijze vermijdt de wetgever dat het toepassingsgebied van de wet al te veel beperkt wordt, en dat de wet vrijwel onmiddellijk achterhaald zou zijn. Niettemin kunnen er wel werkdefinities worden teruggevonden, zij het in de memorie van toelichting.[301] De Raad van State had het echter niet zo begrepen op deze ruime begripsomschrijvingen van de strafbare feiten, en stelde dan ook dat het legaliteitsbeginsel werd geschonden.[302] Toch vind ik, zonder afbreuk te willen doen aan het belang van het legaliteitsbeginsel, dat de wetgever in dit kader een juiste keuze heeft gemaakt. Het nut van een strikte omschrijving ontsnapt mij namelijk enigszins, gezien dit tot gevolg zou hebben dat het toepassingsgebied van de wet daardoor sterk zou worden beperkt, en de termen snel achterhaald zouden zijn. Het gebruik van technologie-neutrale terminologie maakt, naar mijn mening, de kracht uit van deze wet. Gezien cybercriminaliteit zich, net als de technologie zelf, razendsnel ontwikkelt, kreeg men ook na de totstandkoming van de wet te maken met nieuwe fenomenen. Net door de ruime begripsomschrijving werden deze nieuwe fenomenen dan ook onder het toepassingsgebied vervat, dit in tegenstelling tot het geval waarin men had geopteerd voor een strikt begrippenkader.

[301] Wetsontwerp inzake informaticacriminaliteit, *Parl. St.* Kamer, , Memorie van toelichting, 3 november 1999, nr. 213/001,12-13.
[302] T. LAUREYS, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2001, 3-4.

3.2 Bepalingen tot wijziging van het Wetboek van Strafvordering

198. Ook op het niveau van het strafprocesrecht worden er enkele wijzigingen doorgevoerd. De opsporingsdiensten krijgen in dit kader enkele nieuwe bevoegdheden.

3.2.1 Databeslag (artikel 39bis Sv.)

199. Het opsporen van misdrijven in een informatiecontext is niet zo vanzelfsprekend. Het is immers vaak nodig om tijdens een opsporingsonderzoek, of een gerechtelijk onderzoek, gegevens in beslag te nemen. De klassieke inbeslagneming heeft echter enkel betrekking op fysieke goederen, zoals de hele computer, of de harde schijf.[303] De klassieke figuur volstond ook niet meer wanneer de gerechtelijke overheid enkel over de elektronische gegevens wilde beschikken, zonder de materiële goederen in beslag te nemen. Deze situatie was niet houdbaar, gezien ze inefficiënt is, en zorgt voor disproportionele overlast voor de verdachte. Het is met name ondenkbaar dat een onderneming, tijdens een onderzoek, gedurende enkele dagen haar informaticasystemen zou moeten missen.[304]

200. Met het databeslag heeft de wetgever hiervoor, via artikel 7 WIC, een oplossing willen bieden. Het databeslag geeft de procureur des Konings de kans om gegevens te kopiëren, wanneer het beslag van de materiële drager niet nodig is. Vervolgens wordt de toegang tot de elektronische gegevens geblokkeerd, wat neerkomt op de elektronische variant van de verzegeling.[305] Wanneer kopiëren onmogelijk blijkt te zijn, wordt er enkel overgegaan tot de blokkering van de inhoud. De procureur des Konings kan tevens overgaan tot het wissen van de gegevens, indien hij de mening is toegedaan dat de gegevens in strijd zijn met de openbare orde of de goede zeden, of indien ze een risico tot schade opleveren. Er wordt eveneens een beveiligingseis gesteld met het oog op het verzekeren van de integriteit en vertrouwelijkheid van de in beslag genomen data. De ratio legis voor deze beveiligingseis dient gezocht te worden in de vluchtigheid van het medium, evenals het risico dat er ongeoorloofde

[303] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 439.
[304] H. GRAUX, "Wet inzake informaticacriminaliteit.", *ICRI* 2001, http://www.internet-observatory.be.
[305] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 439.

manipulaties zouden plaatsvinden, waardoor de bewijswaarde van de gegevens wordt gecompromitteerd.[306]

3.2.2 Netwerkzoeking (artikel 88ter Sv.)

201. De netwerkzoeking, zoals voorzien door artikel 8 WIC, ligt in het verlengde van de mogelijkheid tot databeslag. De kans is immers reëel dat, indien men bepaalde gegevens in beslag wil nemen, het bronbestand van die data zich niet op dezelfde plaats bevindt als waar het onderzoek wordt gehouden.[307] In een dergelijk geval is het nodig dat de onderzoeksrechter op flexibele wijze kan optreden, en de zoeking van een informaticasysteem moet kunnen uitbreiden naar een informaticasysteem dat zich op een andere plaats bevindt dan diegene waar de zoeking zelf plaatsvindt. Artikel 88ter Sv. voorziet in dit kader een wettelijke grondslag, waardoor de onderzoekers actief op zoek kan gaan naar belangrijke gegevens op een netwerk.[308] Dit alles is wel onderworpen aan voorwaarden. Enerzijds, moet de uitbreiding noodzakelijk zijn om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking en, anderzijds, moeten andere maatregelen disproportioneel zijn, of moet men het risico lopen dat zonder deze uitbreiding bewijselementen verloren gaan.[309] [310] Open netwerken, zoals het internet, komen niet in aanmerking voor een netwerkzoeking, tenzij het als middel wordt gebruikt om een bijzondere toegang tot meer private netwerken te creëren. Algemeen kan er echter gesteld worden dat de onderzoekers zich dienen te beperken tot gesloten netwerken.[311] Gezien de netwerkzoeking een maatregel is die een schending uitmaakt van het recht op privacy, waartoe enkel kan worden overgegaan in de gevallen en onder de voorwaarden door de wet bepaald, is het voor de onderzoeker verboden zijn bevoegdheid te overschrijden.[312] De invoering van de netwerkzoeking leidt dus geenszins tot 'hackende speurders'. In dit kader stelt zich echter een probleem. De onderzoekers zijn slechts gemachtigd te zoeken op plaatsen waar de dader zelf bevoegd was om te komen. De situatie waarin de dader zelf zijn bevoegdheid overschreed, is

[306] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 425.
[307] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 425.
[308] T. LAUREYS, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2002, 64-65.
[309] H. GRAUX, "Wet inzake informaticacriminaliteit.", *ICRI* 2001, http://www.internet-observatory.be.
[310] T. VERBIEST en I. DERVAUX, "La criminalité informatique dans tous ses états", *T.B.H.* 2002, (607) 612.
[311] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 440.
[312] H. GRAUX, "Wet inzake informaticacriminaliteit.", *ICRI* 2001, http://www.internet-observatory.be.

door de wetgever niet voorzien. Dit zorgt voor een hiaat in de wetgeving, vermits het aan het gerecht, volgens de letter van de wet, niet is toegestaan op die plaatsen te gaan zoeken.[313]

202. Een ander aspect van de netwerkzoeking dat de moeite waard is om te onderzoeken is dat van de grensoverschrijdende zoekingen. Internationale netwerken zijn ondertussen immers eerder de regel, dan de uitzondering geworden. De vraag die zich in dit kader dan ook opdringt is onder welke voorwaarden men kan overgaan tot een uitbreiding van de zoeking naar elders gesitueerde systemen. De internationale context waarin vele informaticamisdrijven zich voordoen, kan aanleiding geven tot situaties waarbij bestanden worden opgevraagd die zich in het buitenland bevinden. De wetgever heeft echter gesteld dat dergelijke grensoverschrijdende zoekingen niet als regel kunnen worden beschouwd. Indien de opsporende instanties over voldoende tijd beschikken, dient steeds de weg van de klassieke internationale rogatoire commissies gevolgd te worden.[314] De wetgever heeft echter nagelaten om op concrete wijze te bepalen wanneer gegevens die voortkomen uit grensoverschrijdende zoekingen, gebruikt kunnen worden. De wetgever stelt in dit kader dat er beroep kan gedaan worden op dergelijke gegevens indien deze op een toevallige of onopzettelijke manier werden bekomen. Het optreden van de opsporende diensten dient daarenboven te goeder trouw te zijn.[315] Gegevens die op deze wijze werden bekomen, kunnen enkel worden gekopieerd. De toegang tot deze gegevens, evenals de blokkering of het wissen ervan is niet toegestaan, in tegenstelling tot bij het gewone databeslag. In dit geval is de onderzoeksrechter verplicht dit via het Openbaar Ministerie mee te delen aan het ministerie van Justitie, dat de bevoegde staat hiervan op de hoogte zal stellen.[316] [317] Op deze wijze kan de betrokken staat bepalen of dit al dan niet een inbreuk uitmaakt op hun respectievelijke rechtsorde. De keuze voor de bewoordingen ‘toevallig’ en ‘onopzettelijk’ is in elk opzicht betreurenswaardig te noemen. Beiden impliceren immers een grote appreciatie- en interpretatiemarge. De wetgever gaat hier in zekere zin voorbij aan een rechtlijnige visie.

[313] A. DEBAETS, J. DEENE en N. SENEL, “Cybercriminaliteit”, in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 426.
[314] Omzendbrief van het college van Procureurs-generaal 14 februari 2002, nr. COL 01/2002.
[315] Verslag namens de Commissie voor de Justitie, *Belgische Senaat*, 28 juni 2000, 2-392/3, 78.
[316] J. KEUSTERMANS en F. MOLS, “De wet van 28 november 2000 inzake informaticacriminaliteit: een eerste overzicht”, *R.W.* 2001-2002, (721) 723.
[317] H. GRAUX, “Wet inzake informaticacriminaliteit.”, *ICRI* 2001, http://www.internet-observatory.be.

3.2.3 Medewerkingsverplichting (artikel 88quater Sv.)

203. Artikel 9 WIC heeft de medewerkingsverplichting in het leven geroepen. De ratio legis achter deze bepaling schuilt in het feit dat de opsporende instanties niet steeds over voldoende onderlegd personeel beschikken, men wil als het ware de expertise gaan halen waar ze zit.[318] Concreet worden er twee categorieën van personen bepaald, waar de onderzoeksrechter in dit geval beroep op kan doen. Enerzijds, betreft het de bedieners van het informaticasysteem dat onderzocht wordt, de zogenaamde netwerkbeheerders. Zij kunnen te allen tijde verplicht worden inlichtingen te verschaffen. [319] Anderzijds, kan iedere geschikte persoon die inlichtingen kan verstrekken, worden opgevorderd om zelf bepaalde operaties uit te voeren op een informaticasysteem.[320] [321] [322]

204. De personen, uit beide categorieën, die worden opgevorderd zijn aan geheimhouding onderworpen. Een weigering tot medewerking namens hen leidt tot strafrechtelijke beteugeling, met name een gevangenisstraf van zes maanden tot één jaar en met een geldboete van honderddertig euro tot honderdduizend euro of met een van die straffen alleen. [323] Dit laatste is niet van toepassing op de verdachte zelf, en diens naaste familieleden. Zij kunnen niet tot medewerking verplicht worden, gezien de verdachte over een zwijgrecht beschikt, en er een verbod van zelfincriminatie geldt. Personen met een beroepsgeheim kunnen medewerking weigeren op grond van de gemeenrechtelijk regeling, meer bepaald artikel 458 Sw.[324]

205. Tevens is er voorzien in een regeling waarbij de Belgische staat de aansprakelijkheid draagt voor onopzettelijke fouten van de personen die aan de medewerkingsplicht zijn onderworpen.

---

[318] P. DE HERT en G. LICHTENSTEIN, "Informaticacriminaliteit en het formeel strafrecht", in *CBR Jaarboek* 2002-2003, Antwerpen, Maklu, 2003. (345) 350.
[319] T. LAUREYS, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2002, 83.
[320] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 440.
[321] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 426.
[322] J. DUMORTIER, B. VAN OUDENHOVE en P. VAN EECKE, "De nieuwe Belgische wetgeving inzake informaticacriminaliteit", *Vigiles* 2001, 61.
[323] H. GRAUX, "Wet inzake informaticacriminaliteit.", *ICRI* 2001, http://www.internet-observatory.be.
[324] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 426.

Deze bepaling is uitermate billijk, gezien zij door de staat wordt gedwongen bepaalde handelingen te verrichten.[325]

206. Een kleine, maar niet onbelangrijke, lacune in artikel 88quater Sv. is dat er niet werd voorzien in een vergoeding voor de personen van wie de medewerking wordt opgevorderd. [326] Niet alleen hebben deze personen allicht betere dingen te doen dan steeds kosteloos de staat te dienen, hun motivatie zal daarenboven ongetwijfeld geen hoge toppen scheren.

3.2.4 Aanvullingen van de artikelen 90ter, 90quater en 90septies Sv.

207. Artikel 11 van de WIC zorgt voor een aanzienlijke uitbreiding van artikel 90ter Sv.. Artikel 90ter Sv. voorziet in het afluisteren, kennisname en opname van privé-telecommunicatie tijdens de overbrenging ervan. De lijst van misdrijven waarop artikel 90ter Sv. kan worden toegepast, wordt door artikel 11 WIC uitgebreid met de hierboven besproken nieuwe strafbaarstellingen. Op deze wijze wou de wetgever de opsporende instanties voldoende wapenen om dergelijke misdrijven op een efficiënte wijze op te sporen.[327]

208. Artikel 12 WIC wijzigt dan weer artikel 90quater Sv. Laatstgenoemd artikel voorziet in een afzonderlijke medewerkingsplicht voor telecomoperatoren en dienstverstrekkers in het kader van een tapmaatregel. Net als bij de medewerkingsplicht voorzien in artikel 88quater Sv., wordt hier ook geopteerd voor een strafrechtelijke sanctie in het geval van weigering, evenals een geheimhoudingsplicht.[328]

209. Artikel 13 WIC voert een nieuw lid in bij artikel 90septies Sv. Het nieuwe lid bepaalt dat er, in het kader van een tapmaatregel, ten aanzien van de verworven data passende middelen dienen aangewend te worden teneinde de integriteit en vertrouwelijkheid van de opgenomen communicatie te waarborgen.[329] Wat er exact dient verstaan te worden onder deze passende middelen wordt verduidelijkt in de memorie van toelichting van de WIC. Het gaat

[325] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 426.
[326] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 426.
[327] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 441.
[328] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 441.
[329] H. GRAUX, "Wet inzake informaticacriminaliteit.", *ICRI* 2001, http://www.internet-observatory.be.

meer bepaald om *"technische middelen, en derhalve is de aard daarvan afhankelijk van de stand van de technologie, evenals van de specifieke vereisten van de data. Deze middelen hebben als zodanig geen effect op de bewijswaarde van de data, maar betreffen de modaliteiten van de onttrekking of de bewaring van de data, waardoor nodeloze bewijsbetwistingen voor de rechter kunnen worden voorkomen. Bovendien gaat het hier om een wettelijke vereiste met het oog op het beschermen van het bewijsmateriaal; deze bestaat zelfs niet in het gemeen recht, en werd ingevoegd omwille van de eigenheid van de geïnformatiseerde omgeving."*[330]

3.3 Nieuwe bepalingen in de Belgacomwet

210. Naast de nieuwe strafbaarstellingen en de aanvullingen in het Wetboek van Strafvordering, voert de WIC ook aanpassingen door in de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, ook wel de Belgacomwet genoemd.[331] Meer bepaald betreft het een wijziging van artikel 109ter E van de Belgacomwet. Artikel 14 WIC legt in dit kader aan telecomoperatoren en verstrekkers van telecommunicatiediensten de verplichting op om voor een periode van minimum twaalf maanden de oproep- en identificatiegegevens van hun gebruikers te registreren en te bewaren met het oog op de opsporing en vervolging van strafbare feiten.[332] Deze verplichting, die de bewaringsplicht omschrijft, kon echter niet met onmiddellijke ingang worden toegepast. De Koning diende namelijk deze bepalingen nog verder uit te werken bij Koninklijk Besluit, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. Op 9 januari 2003 werd er een Koninklijk Besluit uitgevaardigd, tot uitvoering van onder andere artikel 109ter E van de Belgacomwet.[333] In dit kader dient men eveneens de wet van 13 juni 2005 betreffende de elektronische communicatie in acht te nemen.[334] De wet van 2005 hief artikel 109ter van de Belgacomwet op, en werd vervangen door nieuwe bepalingen in de wet van 2005. Hierdoor bestond de wettelijke basis van het Koninklijk Besluit niet meer. Het is het

[330] Wetsontwerp inzake informaticacriminaliteit, *Parl. St.*, Kamer, Nr. 213/001, Memorie van toelichting, 3 november 1999, 21-22.
[331] Wet 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.* 27 maart 1991.
[332] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 441.
[333] K.B. 9 januari 2003 tot uitvoering van de artikelen 46bis, §2, eerste lid, 88bis, §2, eerste en derde lid, en 90quater, §2, derde lid van het Wetboek van Strafvordering en van artikel 109ter, E, §2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.* 10 februari 2003.
[334] Wet 13 juni 2005 betreffende de elektronische communicatie, *B.S.* 30 juni 2005.

artikel 126 van laatstgenoemde wet op de elektronische communicatie dat nu de wettelijke basis vormt. De Koning zou door middel van een Koninklijk Besluit de voorwaarden vaststellen waaronder de operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende de regeling van de inlichtingen- en veiligheidsdiensten.[335] [336]

211. In augustus 2009 werden er nieuwe initiatieven afgerond omtrent de vaststelling van de modaliteiten van artikel 126 van de wet van 13 juni 2005. Het project dataretentie had betrekking op de omzetting van de Europese Richtlijn 2006/24/EG. Onder invloed van Vincent Van Quickenborne en Stefaan De Clerck kwamen twee documenten tot stand. Enerzijds, een voorontwerp van wet tot wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van Strafvordering.[337] Anderzijds, kwam een ontwerp van Koninklijk Besluit tot vaststelling van de te bewaren gegevens overeenkomstig artikel 126 van de wet van 13 juni 2005, alsook de voorwaarden en de duur van de bewaring van die gegevens tot stand.[338] Concreet werd een bewaringstermijn van twaalf maanden vooropgesteld. Eind juni 2010 werd de deadline, die werd voorzien voor de goedkeuring van het hele project, gesteld.[339] Deze deadline werd echter niet gehaald door de val van de regering. Geen van beide documenten is dus tot op heden de status van voorontwerp ontgroeid.

212. Nog recenter, op 8 februari 2011, kwam er een Koninklijk Besluit tot stand tot wijziging van het Koninklijk Besluit van 9 januari 2003 tot uitvoering van de artikelen 46bis, § 2, eerste lid, 88bis, § 2, eerste en derde lid, en 90quater, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109ter, E , § 2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Hierin werden echter geen

[335] Artikel 126 wet van 13 juni 2005 betreffende de elektronische communicatie, *B.S.* 30 juni 2005.
[336] Deze laatste zinsnede is ingevoerd door de wet betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten van 4 februari 2010.
[337] http://stefaandeclerck.be.
[338] http://stefaandeclerck.be.
[339] http://www.stefaandeclerck.be.

modaliteiten uitgewerkt aangaande artikel 126 van de wet van 2005. Tot op de dag van vandaag is er dus nog steeds geen sprake van een uitvoeringsbesluit aangaande de dataretentie.

213. Men kan zich in dit kader vragen stellen naar de redenen waarom het zo lang duurt alvorens men een consensus bereikt over een uitvoeringsbesluit van artikel 126 van de wet van 13 juni 2005. De oorzaken hiervoor zijn meervoudig. Eerst en vooral dient er gewezen te worden op het feit dat de Raad van State zich steeds heeft verzet tegen de delegatie aan de Koning.[340] De Raad van State benadrukt meer bepaald dat deze delegatie ongrondwettig is. Laatstgenoemde beroept zich hiervoor op artikel 22 van de Grondwet. Artikel 22 GW bepaalt het volgende: *"Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald."* Oproepgegevens, zoals zij worden beschreven in artikel 126 van de wet van 2005, maken deel uit van het privéleven van de betrokkene. Bijgevolg komt het enkel de wetgever toe te bepalen welke gegevens moeten worden bewaard, evenals de gevallen waarin dergelijke maatregel dient te worden genomen, aldus de Raad van State.[341] Ook de Europese Commissie heeft zich vaak afwijzend opgesteld ten aanzien van de voorziene bewaringsplicht. Volgens laatstgenoemde vormt het artikel in kwestie een inbreuk op de Europese bepalingen omtrent de bescherming van de persoonlijke levenssfeer. Meer algemeen stelt de Commissie dat België in zijn strijd tegen cybercriminaliteit te weinig oog heeft gehad voor de fundamentele rechten en vrijheden.[342] [343] De grootste tegenkanting in dit kader komt uit de hoek van de operatoren, en dat hoeft niet te verbazen. Voor de operatoren brengt de bewaringsplicht immers een forse financiële kost met zich mee. Zij dienen met name aanzienlijke investeringen te doen om aan de gestelde eisen tegemoet te kunnen komen. De bewaartermijn is dan ook het voorwerp geweest van het betere lobbywerk, met aan de ene zijde de opsporende instanties, die een zo lang mogelijke termijn uit de brand wilden slepen, en aan de andere zijde de operatoren, die de bewaringstermijn graag wilden beperken in de tijd.[344]

[340] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (403) 441.
[341] Advies van de Raad van State, *Parl. St.* Kamer, 1999-2000, Nr. 213/001, 56.
[342] J. KEUSTERMANS en F. MOLS, "De wet van 28 november 2000 inzake informaticacriminaliteit: een eerste overzicht", *R.W.* 2001-2002, (721) 732.
[343] J. PAYE, "La loi relative à la criminalité informatique", *Journ. Proc.* 2001, (13) 14.
[344] T. LAUREYS, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2001, 7-8.

3.4 Wijzigingen van de wet van 28 november 2000 inzake informatica-criminaliteit

214. De wet van 28 november 2000 inzake informaticacriminaliteit trad in werking op 13 februari 2001. Op 23 november 2001 zag het Cybercrime-Verdrag van de Raad van Europa het levenslicht. Beide documenten kwam dus ongeveer in hetzelfde tijdsbestek tot stand. België heeft het Cybercrime-Verdrag ondertekend. Om te voldoen aan de verplichtingen bepaald in dit verdrag, drongen zich enkele wetswijzigingen op.[345]

215. Deze wetswijzigingen kwamen er door middel van de wet van 15 mei 2006.[346] De wijzigingen in kwestie resulteerden vooral in een uitbreiding van de bestraffing van informaticacriminaliteit.[347] Initieel werd er ook voorzien in een aantal aanpassingen aan de auteurswet en de genocidewet.[348] Uiteindelijk kwamen deze er echter niet. De wijzigingen die wel werden doorgevoerd, kwamen er na raadpleging van de leden van de Federal Computer Crime Unit. Dit had tot gevolg dat de verbeteringen inhoudelijk sterk waren, waardoor zij zonder veel gepalaver door het parlement zijn geraakt.[349] [350]

216. Vooreerst vond er een aanpassing plaats van artikel 504quater Sw.. Voor de wetswijziging van 15 mei 2006 moest er een effectief vermogensvoordeel verworven worden.[351] Sinds de wetswijziging is het, conform artikel 8 van het Cybercrime-Verdrag, voldoende dat de betrokkene dit beoogt. [352] Het effectief verwerven van een vermogensvoordeel is dus vervangen door het louter opzet. Tot de wet van 15 mei 2006 diende het beoogde economisch voordeel tevens bedrieglijk te zijn. Gezien een vermogensvoordeel an sich bezwaarlijk bedrieglijk kan zijn, werd dit door de wetswijziging dan ook achterwege gelaten. De betrokkene dient met bedrieglijk opzet te handelen, handelingen te goeder trouw zijn niet strafbaar.[353] Verder werd in dit artikel de bewoording

[345] *Parl. St* Kamer 2003-2004, nr. 51-1284/001, 5.
[346] Wet 15 mei 2006 tot wijziging van de artikelen 259bis, 314bis, 504quater, 550bis en 550ter van het Strafwetboek, *B.S.* 12 september 2006.
[347] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 562.
[348] Wetsontwerp tot wijziging van de wet van 28 november 2000 inzake informaticacriminaliteit, de wet van 30 juni 1994 betreffende het auteursrecht en de naburige rechten, en van de wet van 23 maart 1995 tot bestraffing van het ontkennen, minimaliseren, rechtvaardigen of goedkeuren van de genocide.
[349] B. DOCQUIR, "Loi du 15 mai 2006: nouvelles définitions des infractions en matière de criminalité informatique", *RDTI* 2006, (287) 288.
[350] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 563.
[351] http://stefaandeclerck.be.
[352] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 563.
[353] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 565.

'de mogelijke aanwending van gegevens' vervangen door 'de normale aanwending van gegevens'.[354]

217. Vervolgens werd ook artikel 550bis Sw. onder handen genomen. Meer concreet werden de voorbereidingshandelingen, die computerinbraak voorafgaan, aangepakt.[355] Voorheen was er een bijzonder opzet vereist, in de zin dat er een bedrieglijk opzet of een oogmerk om te schaden diende aanwezig te zijn.[356] De wet van 15 mei 2006 bracht hier verandering in, door te stellen dat diezelfde gedragingen op onrechtmatige wijze dienden te geschieden. De bewoordingen 'met bedrieglijk opzet of het oogmerk om te schaden' werden achterwege gelaten. De wet van 15 mei 2006 voegde in de artikelen 550bis en 550ter Sw. eveneens het begrip 'instrumenten' toe, overeenkomstig de bepalingen uit het Cybercrime-Verdrag.[357] Ook de artikelen 259bis en 314bis Sw. werden in dit opzicht gewijzigd.[358]

218. Tenslotte werden ook wijzigingen doorgevoerd op het vlak van de informaticasabotage en datamanipulatie. Sinds de wetswijziging van 15 mei 2006 maakt de wil om te schaden geen constitutief bestanddeel meer uit.[359] Sinds 2006 volstaat het dat de dader schade heeft berokkend, zonder dat voor ogen te hebben gehad, maar wetende dat hij niet gerechtigd was wijzigen aan te brengen.[360] Ook de poging tot datamanipulatie werd vanaf de wet van 15 mei 2006 strafbaar gesteld, terwijl dit voorheen niet het geval was.[361]

219. Op het vlak van het strafprocesrecht hebben er zich geen significante wijzigingen gemanifesteerd.[362]

[354] B. VAN ROY, "Wijzigingen aan de Belgische bepalingen inzake informaticacriminaliteit", *Computerr.* 2006, (314) 314.
[355] http://stefaandeclerck.be.
[356] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 566.
[357] *Parl. St.* Kamer 2003-04, Nr. 51-1284/001, 6.
[358] http://stefaandeclerck.be.
[359] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 567.
[360] F. GOOSSENS, "Wijzigingen in het Belgisch Strafwetboek inzake informaticacriminaliteit", *TVW* 2006, (466) 467.
[361] B. VAN ROY, "Wijzigingen aan de Belgische bepalingen inzake informaticacriminaliteit", *Computerr.* 2006, (314) 314.
[362] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 565.

4. DE BESTRAFFING VAN VERWANTE MISDRIJVEN

4.1 Inleiding

220. De Belgische wetgever heeft door het invoeren van de wet inzake informaticacriminaliteit grote stappen voorwaarts gezet. De vraag blijft echter of de strafwet voldoet om ook a-specifieke informaticacriminaliteit, waarbij het informaticasysteem louter de modus operandi is, te bestrijden. Zijn de klassieke misdrijven met andere woorden zodanig technologieneutraal omschreven, zodat ze ook in een informaticaomgeving kunnen worden toegepast? In dit onderdeel zal er nagegaan worden op welke manier de Belgische strafwet a-specifieke informaticamisdrijven aanpakt.

4.2 Aanranding van de eer of de goede naam

221. Het klassieke vergrijp van de aanranding van de goede eer en de goede naam van personen wordt bestraft door artikel 443 en 444 Sw. De nieuwe mogelijkheden die cyberspace biedt op het gebied van telecommunicatie, zorgen ervoor dat de impact van dit misdrijf aanzienlijk kan vergroten. De vraag stelt zich dan ook of artikel 443 en 444 Sw. voldoende technologieneutraal is omschreven om hieraan het hoofd te kunnen bieden.[363] Dit blijkt echter wel degelijk het geval te zijn.[364]

4.3 Gokken op het internet

222. België beschikt over een zeer stringente regulering omtrent het uitbaten van gokgelegenheden. Op grond van de Kansspelwet[365] geldt er tevens een verbod om spelen, die aan de kenmerken van een kansspel beantwoorden, via het internet, sms of digitale televisie aan te bieden. Overal ter wereld wordt er gepoogd de wildgroei aan cybercasino's in te dijken. Dergelijk casino's zijn ideaal voor het witwassen van opbrengsten verkregen uit illegale activiteiten. Gokken op het internet gaat daarenboven vaak gepaard met inbreuken op de

[363] J. DUMORTIER, B. VAN OUDENHOVE en P. VAN EECKE, "De nieuwe Belgische wetgeving inzake informaticacriminaliteit", *Vigiles* 2001, (44) 53.
[364] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (433) 442.
[365] Wet 7 mei 1999 op de kansspelen, de kansspelinrichtingen en de bescherming van de spelers, *B.S.* 30 december 1999.

privacy regulering. Vaak moet de gokker in kwestie immers allerlei programma's downloaden, waardoor er zich cookies op de harde schijf van de gebruiker gaan nestelen. De meerderheid van de internetservers die kansspelen aanbieden bevinden zich in de Caraïben en in Latijns-Amerika, waar cybercasino's legaal zijn. Het is daarom een zeer moeilijk fenomeen om aan te pakken. Ook is het voor de Belgische wetgever niet evident om de snelle evoluties die zich in dit kader manifesteren, te volgen.[366]

4.4 Oplichting

223. Cyberspace biedt oplichters oneindig veel mogelijkheden om hun activiteiten uit te oefenen. Er zijn tal van voorbeelden waarbij mensen worden opgelicht door bijvoorbeeld mails met de melding dat ze één of andere loterij hebben gewonnen, of dat er een erfenis op hen ligt te wachten.

224. Artikel 496 van het Strafwetboek voorziet in de beteugeling van oplichting. Het toepassingsgebied van dit artikel blijkt ruim genoeg te zijn, waardoor ook fraude op het internet eronder valt. Uit het wetsartikel zelf valt immers af te leiden dat er geen belang wordt gehecht aan het feit dat er al dan niet gebruik wordt gemaakt.

5. EVALUATIE VAN DE WET VAN 28 NOVEMBER 2000 INZAKE INFORMATICA-CRIMINALITEIT

225. België was, tot de totstandkoming van de wet van 28 november 2000, één van de laatste Europese landen waar er geen specifieke wetgeving omtrent informaticacriminaliteit bestond. Dat er nochtans nood was aan dergelijke wetgeving staat als een paal boven water. De 'Bistel'-zaak en de 'ReDaTtacK'-zaak, en de daarbij horende creatieve rechtspraak, hebben deze stelling eens te meer kracht bijgezet.

226. De wetgever heeft uiteindelijk wel de noodzaak aan wetgevende initiatieven in dit kader onderkend, wat heeft geleid tot het ontstaan van de wet inzake informaticacriminaliteit. Waar België voor de totstandkoming van de wet nog helemaal achterop hinkte, hees het zich in 2000 weer op naar een meer respectabelere positie. De wet inzake informaticacriminaliteit

[366] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (433) 443.

was dan ook, inhoudelijk gezien, best wel een toonbeeld van degelijke regelgeving. De nieuwe strafbaarstellingen correspondeerden, behoudens enkele kleine aanpassingen achteraf, grotendeels met de bepalingen uit het Cybercrime-Verdrag. Hetzelfde kan gezegd worden wat betreft de nieuwigheden aangaande het strafprocesrecht. Bij dit laatste aspect dienen wel twee kanttekeningen te worden geplaatst. De eerste kanttekening heeft betrekking op de netwerkzoeking. Opsporingsdiensten zijn in dit kader slechts gemachtigd om te zoeken op plaatsen waar de dader zelf bevoegd was om te komen. Het geval waarin de dader zelf zijn bevoegdheden overschreed, werd door de wetgever niet voorzien. Tevens kunnen er zich problemen stellen bij internationale netwerkzoekingen. De regeling hieromtrent is niet de meest duidelijke, waardoor inbreuken op de soevereiniteit van andere landen niet ondenkbaar zijn. De tweede kanttekening heeft betrekking op artikel 109ter E van de Belgacomwet, waar nog steeds geen uitvoeringsbesluit voor tot stand is gekomen.

Hoofdstuk 3: Implicaties van het Cybercrime-verdrag op het vooronderzoek

1. INLEIDING

227. Het Cybercrime-Verdrag en de wet van 28 november 2000 kwamen ongeveer tegelijkertijd tot stand. De Belgische wet heeft na verloop van tijd enkele subtiele wijzigingen ondergaan, om conform te zijn aan het Cybercrime-Verdrag. Een belangrijke vraag in dit kader is in welk opzicht het Cybercrime-Verdrag al dan niet een invloed heeft gehad op het Belgische vooronderzoek. De uitdagingen in het kader van informaticacriminaliteit liggen, volgens velen, niet zozeer op het vlak van het materieel strafrecht, maar eerder op het vlak van de opsporing en de handhaving.[367] In dit hoofdstuk zal er op deze materie dieper worden ingegaan, door de desbetreffende bepalingen uit beide teksten met elkaar te vergelijken.

2. HET VASTLEGGINGSBEVEL

228. Het Cybercrime-Verdrag regelt in artikel 16 en 17 het relatief nieuwe opsporingsmiddel van het vastleggingsbevel. Het vastleggingsbevel vormt geen opsporende bevoegdheid in de

[367] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", *Vigiles* 2004-05, (153) 153.

letterlijke zin van het woord. Het dient eerder beschouwd te worden als een faciliterend instrument.[368] In die zin dat het vastleggingsbevel toelaat dat klassieke maatregelen voor de verzameling van gegevens, zoals de huiszoeking en de inbeslagname, op een efficiënte en doelgerichte wijze kunnen worden uitgeoefend.[369] Artikel 16 van het Cybercrime-Verdrag voorziet in een dubbele verplichting. Enerzijds, wordt er een bewaringsplicht opgelegd en, anderzijds, een integriteitsplicht. Artikel 17 van datzelfde verdrag verduidelijkt de situatie wanneer het bevel betrekking heeft op verkeersgegevens.

229. De Belgische situatie in dit kader is licht afwijkend van het bovenstaande. België heeft met name geen volwaardig vastleggingsbevel opgenomen in haar rechtsbestel, maar wel een algemene bewarings- en integriteitsplicht.[370] Deze bepalingen zijn opgenomen in artikel 109ter, E van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Artikel 109ter, E heeft, net zoals de bepalingen in het Cybercrime-Verdrag, niet de ambitie om een nieuwe opsporingsmaatregel in het leven te roepen. Net als de bepalingen in het verdrag, strekt de bepaling ertoe andere opsporingsmaatregelen te vergemakkelijken. In het Belgische kader handelt het dan over de artikelen 46bis, 88bis en 90ter van het Strafwetboek. Een markant verschil tussen het Cybercrime-Verdrag en de Belgische regulering in kwestie is de periode waarvoor de plicht geldt. Waar het verdrag voorziet in een termijn van negentig dagen, eist de Belgische wetgever niet minder dan twaalf maanden, als minimum.[371] Een ander verschil tussen beide teksten situeert hem in het feit dat de Belgische wetgever de plicht oplegt ten aanzien van internettoegangsleveranciers en netwerkoperatoren, daar waar het Cybercrime-Verdrag zicht richt tot elke persoon die verkeersgegevens en data ter beschikking heeft.[372]

[368] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", *Vigiles* 2004-05, (153) 155.
[369] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", *Vigiles* 2004-05, (153) 155.
[370] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", Vigiles 2004-05, (153) 156.
[371] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", Vigiles 2004-05, (153) 156.
[372] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", Vigiles 2004-05, (153) 156.

3. HET OVERLEGGINGSBEVEL

230. Artikel 18 en 19 van het Cybercrime-Verdrag voorzien respectievelijk in een overleggings- en een medewerkingsbevel. Het overleggingsbevel uit artikel 18 heeft enkel betrekking op opgeslagen of bestaande gegevens, waardoor zogenaamde traffic-data ongemoeid worden gelaten. Artikel 19 van het verdrag heeft eveneens enkel betrekking op bestaande gegevens.[373] De vraag die zich in dit kader stelt is wie nu juist het bevel kan geven om tot deze maatregelen over te gaan. Het Cybercrime-Verdrag heeft dit niet concreet uitgewerkt, het stipuleert wel dat dit moet worden nagegaan op nationaal niveau, met inachtneming van de rechtsbescherming. Hoe groter de impact van de maatregel is, hoe hoger men in die hiërarchie dient te gaan.[374] Artikel 19 bepaalt verder dat alleen data in overeenstemming met de billijkheid moeten overlegd worden, die informatie moet met andere woorden noodzakelijk zijn voor de uitvoering van een huiszoeking of beslag.[375]

231. Naar Belgisch recht zijn er twee bepalingen die voorzien in soortgelijke verplichtingen, artikel 88quater en artikel 90quater Sv. Artikel 88quater Sv. bepaalt twee categorieën van personen, op wie de onderzoeksrechter beroep kan doen. Enerzijds, betreft het de bedieners van het informaticasysteem dat onderzocht wordt, de zogenaamde netwerkbeheerders. Zij kunnen te allen tijde verplicht worden inlichtingen te verschaffen. Anderzijds, kan iedere geschikte persoon die inlichtingen kan verstrekken, worden opgevorderd om zelf bepaalde operaties uit te voeren op een informaticasysteem.[376] [377] Artikel 88quater Sv. verschilt, eerst en vooral, wat betreft de opbouw van de gelijksoortige bepaling van het Cybercrime-Verdrag. De Belgische norm is geformuleerd als antwoord op de encryptieproblematiek, een gegeven waar artikel 18 van het verdrag niet op gericht is. Verder stelt artikel 88quater Sv. de weigering van medewerking strafbaar, terwijl het verdrag daar als dusdanig geen gewag van maakt. Ook maakt de Belgische norm een onderscheid tussen twee categorieën van personen van wie medewerking kan worden gevorderd. Deze opsplitsing komt in het Cybercrime-

[373] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", Vigiles 2004-05, (153) 160.
[374] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", *Vigiles* 2004-05, (153) 160.
[375] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", *Vigiles* 2004-05, (153) 159.
[376] A. DEBAETS, J. DEENE en N. SENEL, "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, (381) 426.
[377] J. DUMORTIER, B. VAN OUDENHOVE en P. VAN EECKE, "De nieuwe Belgische wetgeving inzake informaticacriminaliteit", *Vigiles* 2001,(44) 61.

Verdrag niet voor. Tenslotte is er in artikel 88quater Sv. geen werk gemaakt van een soort billijkheidsclausule, die wel terug te vinden is in het Cybercrime-Verdrag. De Belgische wetgever heeft in artikel 90quater Sv daarenboven nog voorzien in een bijkomende medewerkingsplicht, gericht aan telecomoperatoren en dienstverstrekkers. Van hen kan medewerking worden gevorderd in het kader van een tapmaatregel. [378] Een dergelijke, verdere opsplitsing, wordt niet voorzien in het Cybercrime-Verdrag, maar valt niettemin te beschouwen als zijnde een goed initiatief van de Belgische wetgever.

4. DE NETWERKZOEKING EN INBESLAGNAME

232. Artikel 19 van het Cybercrime-Verdrag voorziet de mogelijkheid om computersystemen en opslagmedia te doorzoeken en de daarop gevonden gegevens in beslag te nemen. Concreet betreft het dus een mogelijkheid tot netwerkzoeking, al komt dit begrip zelf niet voor in het verdrag, en databeslag. [379] Het verdrag specifieert dat de netwerkzoeking enkel mag uitgevoerd worden door hiervoor bevoegde opsporingsdiensten. Het databeslag dient dan weer uitgevoerd te worden door de organen belast met het onderzoek zelf.[380] Het databeslag heeft, naar de geest van het Cybercrime-Verdrag, twee doelen. Enerzijds, het verzamelen van gegevens en, anderzijds, het beslag leggen op diezelfde gegevens, om ze vervolgens ontoegankelijk te maken of te verwijderen.

233. De bepalingen omtrent de netwerkzoeking en het databeslag zijn in het Belgisch recht terug te vinden in de artikelen 88ter en 39bis Sv. In tegenstelling tot de bepaling in het verdrag, wordt er in het Wetboek van Strafvordering geen specifieke aandacht geschonken aan de zoeking in een computersysteem tijdens een huiszoeking. [381] Artikel 88ter gaat onmiddellijk uit van de situatie waarin er een uitbreiding van de huiszoeking benodigd is. Het valt te betreuren dat de wetgever hier aan voorbijgaat, eens te meer omdat dit, met het oog op de praktische uitwerking, enkele onduidelijkheden met zich meebrengt.[382] Men kan zich met

[378] S. VANSTEENHUYSE en P. T'JONCK, "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, (433) 441.
[379] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", *Vigiles* 2004-05, (153) 162.
[380] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", Vigiles 2004-05, (153) 164.
[381] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", Vigiles 2004-05, (153) 163.
[382] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", Vigiles 2004-05, (153) 163.

name de vraag stellen of er op basis van één huiszoekingsbevel kan overgegaan worden tot een netwerkzoeking, of de onderzoeksrechter de opdracht dient te specifiëren op het bevel zelf, wat er dient gedaan te worden indien een gsm of portable in beslag wordt genomen buiten de gevallen van een huiszoeking, en of men over een huiszoekingsbevel dient te beschikken om bijvoorbeeld een voicemail te beluisteren?[383]

234. Wat de rechtsbescherming betreft bepaalt artikel 39bis Sv. dat er in het geval van databeslag een notificatieplicht geldt, waarbij de onderzoeksrechter de verantwoordelijke van het informaticasysteem op de hoogte dient te brengen. Hier gaat de Belgische wetgever verder dan het Cybercrime-Verdrag, dat geen dergelijke notificatieplicht in het leven roept.[384]

5. DE INTERNATIONALE NETWERKZOEKING

235. Zoals voorafgaand reeds werd vermeld, wordt de netwerkzoeking geregeld door artikel 19 van het Cybercrime-Verdrag. Gezien cybercrime zich vaak manifesteert over de landsgrenzen heen, stelt zich de vraag naar de internationale netwerkzoeking. Het Cybercrime-Verdrag specifieert echter niets over een grensoverschrijdende zoeking en inbeslagname, naast de geijkte kanalen van de rechtshulp in strafzaken. De netwerkzoeking is, in dit kader, enkel mogelijk voor computersystemen die zich op het eigen grondgebied bevinden. Artikel 32 laat in uitzonderlijke gevallen wel toe dat opsporingsdiensten eenzijdig gegevens benaderen die zijn opgeslagen op computersystemen buiten het nationale grondgebied.

236. De Belgische wetgever is op dit onderwerp wel dieper ingegaan. Artikel 88ter Sv. voorziet namelijk ook in de netwerkzoeking voor gegevens die zich in het buitenland bevinden. Het betreft dan enkel de mogelijkheid tot kopiëren, de vernietiging of het onbruikbaar maken van de data is niet mogelijk. Bijkomend dient de onderzoeksrechter dit mee te delen aan de minister van Justitie, die de overheid van de betrokken staat op de hoogte dient te brengen. Deze manier van werken mag echter niet beschouwd worden als de regel, in eerste instantie dient men steeds de weg van de internationale rogatoire commissies te bewandelen. De Belgische wetgever is hier opmerkelijk verder gegaan dan het Cybercrime-

[383] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", Vigiles 2004-05, (153) 163.
[384] P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", *Vigiles* 2004-05, (153) 164.

Verdrag. Waar het verdrag bepaalt dat onderzoekers eerst moeten nagaan of er verdragsrechtelijke of wettelijke gronden voorhanden zijn die de buitenlandse zoeking legitimeren, is dit in de Belgische context niet het geval. De onderzoeksrechter heeft in dit kader dan ook erg ruime bevoegdheden. Niet alleen beschikt hij over een universele bevoegdheid, ook van stopzetting is er nergens sprake.

Hoofdstuk 4: De opsporing van cybercriminaliteit in België

1. INLEIDING

237. De wet van 28 november 2000 inzake de informaticacriminaliteit vormt een degelijke basis voor de aanpak van cybercrime. Adequate wetgeving is in dit kader zeker een belangrijk punt, maar misschien nog belangrijker is de wijze waarop de wet in praktijk wordt toegepast. In dit hoofdstuk zal worden nagegaan hoe in België de opsporing van cybercriminelen verloopt.

2. DE BELGISCHE OPSPORINGSINSTANTIES

2.1 Algemeen kader

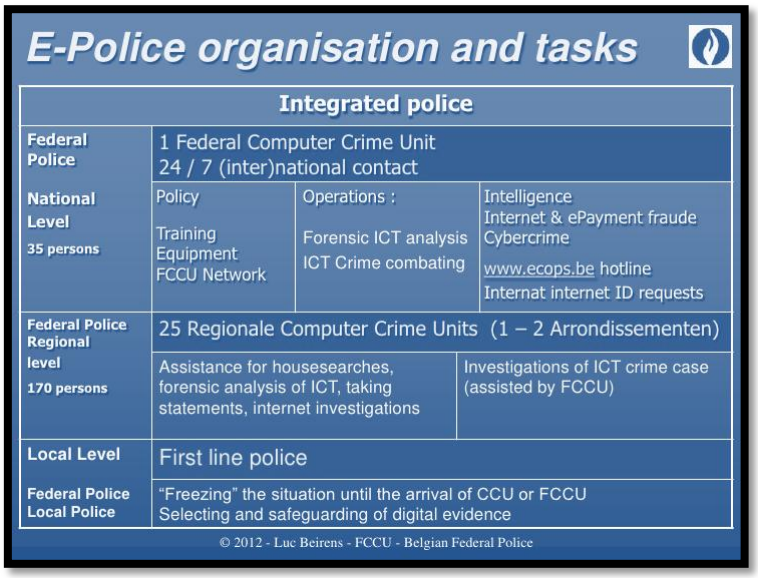
238. Midden de jaren ’90 vond er een snelle stijging van het gebruik van informatica en telecommunicatie plaats. Deze evolutie ging eveneens gepaard met een snelle stijging van het aantal hieraan gelieerde delicten. Er werd op dat punt dan ook besloten tot de oprichting van gespecialiseerde diensten, wiens hoofddoel eruit bestond deze criminaliteit aan te pakken.[385]

239. Begin de jaren ’90 werden de Computer Crime Units van de Gerechtelijke Politie opgericht. In 1995 werd in de schoot van de toenmalige Rijkswacht het Team voor Bijstand en Opsporingen in Geautomatiseerde Omgevingen (BOGO) opgericht.[386] In 1997 kreeg de

[385] Omzendbrief van het College van Procureurs-generaal 16 april 1999 betreffende de Ministeriële richtlijn van 16 maart 1999 tot regeling van de samenwerking, coördinatie en taakverdeling tussen de lokale politie en de federale politie inzake de opdrachten van de gerechtelijke politie, nr. COL 6/99.
[386] B. BEIRENS, “Op zoek naar criminele bits, digitaal rechercheren”, *Politeia* 1998, (9) 10.

Nationale Brigade van de Gerechtelijke Politie een National Computer Crime Unit.[387] De wet op de politiehervorming[388] heeft dit landschap ingrijpend veranderd. Het BOGO-team van de Rijkswacht smolt samen met de National Computer Crime Unit van de Gerechtelijke Politie. Door deze samensmelting zag de Federal Computer Crime Unit het levenslicht. De regionale Computer Crime Units bleven bestaan. De politiediensten gespecialiseerd in het forensisch onderzoek van informatica- en telecommunicatiesystemen en de strijd tegen cybercriminaliteit, zijn dus uitgebouwd op twee niveaus. Enerzijds, zijn er de RCCU's binnen de gedeconcentreerde gerechtelijke politie. Anderzijds, de FCCU op nationaal niveau binnen de directie DJF. [389] Schematisch gezien levert dat volgende situatie op:

FIGUUR 4: ALGEMEEN OVERZICHT OPSPORINGSINSTANTIES[390]



2.2 Regional Computer Crime Units (RCCU)

240. Op het niveau van de gerechtelijke arrondissementen bevinden zich de Regional Computer Crime Units. Er zijn 25 RCCU's, onder leiding van de gerechtelijke directeurs. De RCCU's beschikken over 170 personeelsleden, waarvan er een twintigtal administratief werk

[387] V. SENNESAEL, "National Computer Crime Unit: digitale flikken", *Computer Magazine* 2000, (73) 73.
[388] Wet 7 december 1998 tot organisatie van een geïntegreerde politiedienst, *B.S.* 8 januari 1999.
[389] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 23.
[390] www.slideshare.net/LucBeirens/20120329-infosecurity-bru.

verrichten.[391] De RCCU's staan in voor de garantie op een kwalitatief forensisch ICT-onderzoek van pc-apparatuur, andere gegevensdragers en kleine netwerken.[392]

241. Meer concreet staan de RCCU's de politiediensten in hun bevoegdheidsgebied bij wat betreft:[393]

- het uitvoeren van zoekingen op ICT-systemen binnen het kader van huiszoekingen;
- het forensisch onderzoek van in beslag genomen ICT-materiaal;
- het verhoor van getuigen of verdachten in ICT-gebonden materies of misdrijven;
- het opsporen van verdachten of hun sporen op publieke netwerken;
- het verstrekken van operationeel advies aan gerechtelijke en politiële overheden.

242. In april 2012 heeft het kernkabinet het licht op groen gezet voor een diepgaande hervorming van het gerechtelijk landschap. Deze hervorming impliceert het terugschroeven van de gerechtelijke arrondissementen van zevenentwintig naar twaalf.[394] Wat de implicaties van deze hervorming zullen zijn ten aanzien van de RCCU's valt af te wachten. Het is niet ondenkbaar dat het aantal RCCU's eveneens flink zal teruggeschroefd worden.

2.3 Federal Computer Crime Unit (FCCU)

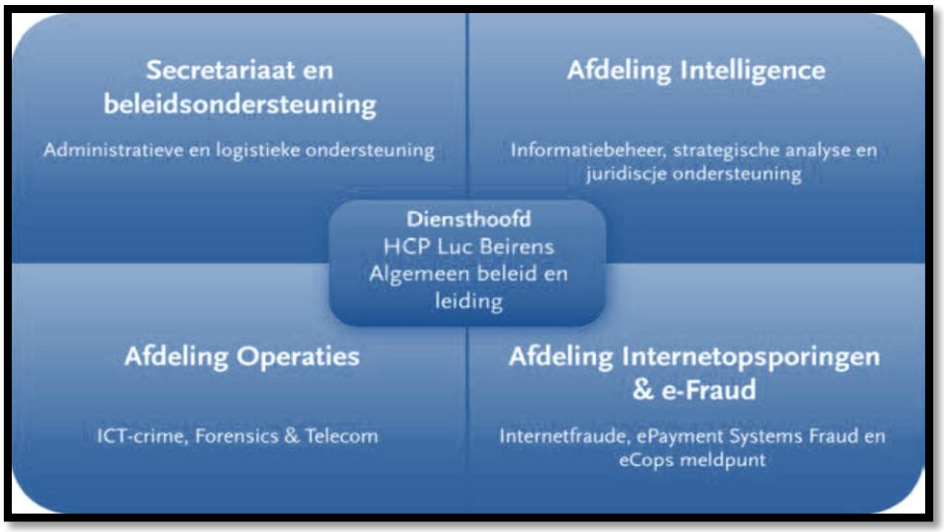
243. De Federal Computer Crime Unit maakt de federale component uit, en ressorteert binnen de Directie ter bestrijding van de economische en financiële criminaliteit. De FCCU staat sinds 2001 onder leiding van Luc Beirens.

2.3.1 Organisatie

244. De FCCU is onderverdeeld in vier secties, met name de secties internetopsporingen, operaties en intelligence. Deze drie secties worden bijgestaan door de dienst secretariaat en beleidsondersteuning, die voorzien in een administratieve en logistieke ondersteuning.[395]

[391] Zie bijlage 'interview met Luc Beirens'.
[392] www.polfed-fedpol.be/org/org_dgj_FCCU_RCCU_nl.php.
[393] L. BEIRENS, *Informatiefiche inzake de organisatie en werking van de Federal Computer Crime Unit (FCCU) en de Regional Computer Crime Units (RCCU)*, Brussel, 2007, 2-3.
[394] X. "Aantal gerechtelijke arrondissementen daalt naar twaalf", *Knack* 17 april 2012, www.knack.be.
[395] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 23.

FIGUUR 5: ORGANISATIEKADER FCCU [396]



- *Sectie Opsporingen*: deze sectie houdt zich bezig met Internetfraude, en meer algemeen met de operationele bijstand bij internetopsporingen, evenals het beheer van het eCops loket;
- *Sectie Intelligence*: deze sectie houdt zich bezig met het informatiebeheer, evenals de strategische analyse en juridische ondersteuning;
- *Sectie Operaties*: deze sectie fixeert zich op ICT-crime in het algemeen. Zij zorgt voor gespecialiseerde steun aan de centrale operationele opsporingsdiensten en de RCCU's, evenals voor onderzoek van ICT-systemen in het kader van meer traditionele criminaliteit;
- *Secretariaat en Beleidsondersteuning*: deze afdeling staat in voor administratieve en logistieke ondersteuning. Meer bepaald richten zij zich op het algemeen advies inzake ICT-onderzoek, de aankoop van materiaal en de opleiding van personeel.

2.3.2 Strategische doelstellingen

245. Cybercrime is een steeds meer voorkomend fenomeen. Het Nationaal Veiligheidsplan 2004-2007 heeft als eerste document een aantal strategische doelstellingen geformuleerd, die dienen nagestreefd te worden in de strijd tegen informaticacriminaliteit.[397] De doelstellingen

[396] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 24.
[397] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Vijfde Activiteitenverslag 2006, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 53.

zijn gericht naar de gespecialiseerde politiediensten, met name de FCCU en de RCCU's. De doelstellingen zijn de volgende:

- de detectie van ICT-criminaliteit en misbruik verhogen en het beeld hiervan verbeteren;
- de traceerbaarheid van daders en hun sporen in cyberspace verbeteren;
- dreigingen op de werking van ICT-infrastructuren in vitale overheids- en bedrijfssectoren voorkomen of beperken;
- de veiligheid op het internet verhogen;
- snel en efficiënt tussenbeide komen bij ICT-criminaliteit.

246. Het Nationale Veiligheidsplan 2012-2015 heeft in dit kader vastgehouden aan diezelfde strategische doelstellingen, en beschouwt informaticacriminaliteit als een prioritair criminaliteitsfenomeen.[398]

2.3.3 Activiteitsdomeinen

247. De FCCU richt zich op informaticacriminaliteit, met als doel de burgers te beschermen tegen alle vormen van traditionele en nieuwe criminaliteitsfenomenen. De FCCU fungeert in dit kader als nationaal en internationaal aanspreekpunt. De Federal Computer Crime Unit werkt dan ook samen met de partners van BelNIS, met het oog op een nationale strategie voor de beveiliging van informaticasystemen, met speciale aandacht voor deze van de overheid, en kritieke infrastructuren.[399] Dit maakt de hoofdmoot uit van de activiteiten van de FCCU, de meeste aandacht gaat naar het voorkomen en bestrijden van aanvallen op kritiek infrastructuren.[400] Indien men erin zou slagen de netwerken van deze infrastructuren lam te leggen, bestaat er een reëel risico op economische problemen.[401]

248. Sinds 2007 focust de FCCU zich tevens op alles wat e-banking misdrijven betreft. Het betreft dan vooral phishingwebsites, evenals het infecteren van de eindgebruiker waardoor

[398] www.polfed-fedpol.be/pub/pdf/NVP2012-2015.pdf.
[399] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 24.
[400] Zie bijlage 'interview met Luc Beirens'.
[401] Zie bijlage 'interview met Luc Beirens'.

zijn pc in een botnet komt te staan.[402] Op het moment dat de gebruiker naar zijn bankwebsite gaat, krijgt de cybercrimineel een melding. Op dat moment komt de crimineel op de verbinding van de gebruiker, waardoor de crimineel tevens transacties kan doen. De crimineel heeft op dat punt wel de medewerking van de gebruiker nodig om de transactie te kunnen voltooien. Via allerlei kunstgrepen probeert de crimineel de gebruiker zover te krijgen dat hij de transactie dan uiteindelijk met zijn digipass bevestigt.[403]

249. Een ander fenomeen, waar de FCCU recent mee wordt geconfronteerd, is zogenaamde 'ransomware'. Dit houdt in dat de cybercriminelen een pc hacken en hem onbruikbaar maken. De gebruiker krijgt dan een melding dat hij een bepaald bedrag dient over te maken om de blokkering op te heffen.[404]

250. De Federal Computer Crime Unit levert bovendien gespecialiseerde steun aan centrale opsporingsdiensten, in het kader van een onderzoek van ICT-systemen bij traditionele vormen van criminaliteit.[405] Eveneens wordt er steun verleend aan de RCCU's bij dossiers inzake informaticacriminaliteit en telecommunicatiefraude.[406]

251. Tevens wordt er onderzoek verricht naar nieuwe informaticasystemen, forensische onderzoeksprogramma's en nieuwe platformen op het internet zoals sociale netwerksites, chatplatformen, netwerken voor bestandsuitwisseling, e.d..[407]

252. De FCCU besteed eveneens aandacht aan de bestrijding van klassieke vormen van criminaliteit, die zich voordoen via het internet.[408] In dit kader werkt de FCCU samen met de FOD Economie, via eCops, het meldpunt voor internetgerelateerde criminaliteit.[409]

[402] Een botnet is een groep van computers die besmet zijn met malware (kwaadaardige software). Via deze malware kan een phisher de controle uitoefenen over verschillende computers en kan hij verborgen blijven op het Internet omdat hij opereert via de computers van andere mensen.
[403] Zie bijlage 'interview met Luc Beirens'.
[404] Zie bijlage 'interview met Luc Beirens'.
[405] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 24.
[406] Zie bijlage 'interview met Luc Beirens'.
[407] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 24.
[408] Zie bijlage 'interview met Luc Beirens'.
[409] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 24.

253. Verder zet de FCCU samenwerkingsverbanden op met nationale en internationale partners voor de identificatie van internetgebruikers bij internationale operatoren, zoals Microsoft en Google.[410]

254. De FCCU organiseert tevens op regelmatige basis informatiesessies, zowel voor politieopleidingen zelf, als voor hogescholen, universiteiten en bedrijven.[411] Op deze wijze wil de FCCU haar verworven kennis uitdragen, en op een proactieve wijze bijdragen tot de voorkoming van informaticacriminaliteit.[412]

255. Tenslotte zet de FCCU zich in voor de beeldvorming van de fenomenen van informaticacriminaliteit. Zo poogt de FCCU nationale en internationale internetfraude in kaart te brengen.[413]

2.3.4 Budget

256. Het is een publiek geheim dat de FCCU niet ruim bemeten is als het op budget aankomt. Dit is reeds sinds het ontstaan van de FCCU een heikel punt. Niettemin worden er wel financiële inspanningen gedaan, al brengen deze echter niet veel zoden aan de dijk. Zo heeft de federale gerechtelijke politie in 2010 een investeringsbudget van 531.000 euro ter beschikking gesteld voor de aankoop van specifiek forensisch ICT-onderzoeksmateriaal. Het doel van deze investering was tweeledig. Enerzijds, werd beoogd afgeschreven materiaal te vervangen en, anderzijds, had dit tot doel het personeel te voorzien van nieuw materiaal. Zo werden er software-updates voor forensische analyse van pc's aangekocht, evenals een server voor visualisatie van infrastructuur en een werkstation met de nodige software en harddisks voor alle operationele Computer Crime Unit-leden.[414]

257. Ook de federale overheidsdienst Justitie deed in datzelfde jaar een duit in zakje. Ongeveer 200.000 euro werd vrijgemaakt voor de aankoop van gegevensdragers. Justitie

[410] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 25.
[411] Zie bijlage 'interview met Luc Beirens'.
[412] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 25.
[413] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 25.
[414] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 15.

maakt deze investering, die buiten de politiebegroting valt, gezien die gegevensdragers een bewijsstuk in strafzaken kunnen uitmaken. [415]

2.3.5 Personeel

258. Dat de Computer Crime Units met een personeelstekort kampen, is een algemeen gekend oud zeer. Bij de FCCU zijn er heden ten dage vijfendertig personen tewerkgesteld, waarvan er tien administratief werk verrichten.[416] Dit gebrek kan enigszins opgevangen worden door investeringen te doen in infrastructuur, waardoor men meer kan doen met minder mensen. In dat opzicht heeft de FCCU dan ook inspanningen gedaan om hieraan tegemoet te komen. Meer bepaald werd een programma ontwikkeld, genaamd 'Forensic Robust Investigation Toolkit', om gegevens op een gelijktijdige en geautomatiseerde wijze op te vragen in functie van de behoeften van de onderzoekers.[417] Op deze wijze wordt er kostbare tijd gewonnen, zowel voor de leden van de FCCU als voor de traditionele opsporingsdiensten.[418]

2.3.6 Samenwerking met niet-politionele diensten

259. Om haar doelstellingen te bereiken staat de FCCU er niet alleen voor. Er zijn tal van samenwerkingsverbanden die het werk van de FCCU vergemakkelijken en ondersteunen, zowel met politionele als niet-politionele instanties. Enkele van deze samenwerkingsverbanden met niet-politionele diensten zullen in dit verband besproken worden.

2.3.6.1 ISPA

260. Een eerste niet-politionele organisatie die een aanzienlijk belang heeft in het kader van de strijd tegen cybercriminaliteit is de ISPA. Wat de Internet Service Providers Association juist is, werd reeds eerder besproken.[419] In deze setting is de ISPA vooral belangrijk omwille

[415] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 15.
[416] Zie bijlage 'interview met Luc Beirens'.
[417] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 24.
[418] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 24.
[419] Voor meer uitleg omtrent de werking van de ISPA, verwijs ik u naar p9 e.v..

van het samenwerkingsprotocol van 28 mei 1999, dat gesloten werd tussen de ISPA en de overheid.[420] Dit protocol strekt ertoe de Internet Service Providers te verplichten om bij misbruiken onmiddellijk het meldpunt eCops op de hoogte te stellen. Verder verplicht dit protocol de ISP's met de gerechtelijke instanties samen te werken, evenals de identificatiegegevens van zijn klanten kenbaar te maken, indien daarom wordt gevraagd.

2.3.6.2 CERT

261. Het CERT is het Belgisch Nationaal Computer Emergency Response Team. Het CERT is uitgebaat door BELNET, het Belgisch nationaal onderzoeksnetwerk, in opdracht van Fedict en in samenwerking met het BIPT.[421] Het is een publieke dienst die de Belgische bevolking wil voorzien van informatie rond computerbeveiliging. Het doelpubliek van het CERT zijn de particulieren die thuis internet gebruiken, evenals de aanbieders van belangrijke en kritieke infrastructuur.[422] Vooral wat dat laatste betreft dienen we een overlapping op te merken met de actieradius van de FCCU. Beiden werken in dat opzicht dan ook samen. Het CERT is in zekere zin een experimenteel gegeven, en heeft zijn plaats nog niet volkomen verworven.[423] Het CERT heeft geen politiebevoegdheid, maar kan in dit verband rekenen op een goede samenwerking met de FCCU.[424]

2.3.6.3 BIPT

262. Het Belgisch Instituut voor postdiensten en telecommunicatie, kortweg BIPT, vervult ook een rol in de strijd tegen cybercriminaliteit. De bevoegdheid van het BIPT is tweeledig.[425] De eerste bevoegdheid slaat op de nieuwe regulerende opdrachten op de geliberaliseerde telecommunicatiemarkten. Het BIPT neemt de nodige maatregelen opdat het regelgevingskader wordt nageleefd, de concurrentie zich ten volle en billijk kan ontplooien, sommige opdrachten van openbaar nut worden vervuld en de consumentenbelangen worden gevrijwaard. De tweede bevoegdheid heeft betrekking op de uitoefening van een soeverein gezag op specifieke technische gebieden. Sommige hulpmiddelen, zoals het

[420] www.ispa.be.
[421] www.cert.be.
[422] https://www.cert.be.
[423] Integraal Verslag met vertaald beknopt verslag van de toespraken, *Parl. St.* Kamer 2011-12, nr. criv 53 com, www.dekamer.be/doc/CCRI/pdf/53/ic361.pdf, 361.
[424] Integraal Verslag met vertaald beknopt verslag van de toespraken, *Parl. St.* Kamer 2011-12, nr. criv 53 com, www.dekamer.be/doc/CCRI/pdf/53/ic361.pdf, 361.
[425] http://www.bipt.be.

elektromagnetisch spectrum of de nummervoorraad, zijn schaars: er is een regulator nodig om het gebruik nauwkeurig te verdelen, te reglementeren en te controleren. Het instituut vervult nog andere technische opdrachten van openbaar belang.[426]

2.3.6.4 Spamsquad-werkgroep

263. Spamsquad is een informele werkgroep, bestaande uit mensen uit de academische wereld, overheidsvertegenwoordigers, rechtsgeleerde en professionelen uit de sector. Spamsquad buigt zich over methodes om spam te meten en over de uitwerking van gemeenschappelijke oplossingen om het fenomeen actief te bestrijden.[427] Het hoofddoel van deze werkgroep is bewustzijn creëren bij de bevolking omtrent het gegeven spam.

2.3.6.5 BelNIS-werkgroep

264. De werkgroep BelNIS werd eind 2005 boven de doopvont gehouden. De regering ging over tot oprichting van dit overlegplatform voor informatieveiligheid, op voorstel van het Comité voor Inlichting en Veiligheid. Het doel ervan is alle overheidsdiensten en andere partijen samen te brengen rond de beveiliging van geclassificeerde informatie en de beveiliging van kritieke ICT-infrastructuur. De toenmalige minister van Werk en Informatisering, Peter Vanvelthoven, en de FCCU waren de stuwende krachten achter de oprichting van dit platform, dat in 2006 van start ging.[428]

2.3.7 De FCCU en de opsporing

265. De meeste zaken waar de FCCU een rol in speelt, kennen hun oorsprong in de vorm van een klacht, waarna de onderzoeksrechter instructies overmaakt aan de FCCU. De FCCU heeft in principe geen autonome opsporingsbevoegdheid. In de meeste gevallen gaan de burgers naar de lokale politie om klacht neer te leggen, waar er vervolgens een dossier wordt gestart. Voor deze lokale misdrijven wordt dan de lokale recherche ingeschakeld. Eens dit arrondissements overstijgend is gaat men over naar de federale recherche. De federale gerechtelijke politie is op twee niveaus opgesplitst, waarbij de centrale diensten ondersteuning

[426] http://www.bipt.be.
[427] http://www.spamsquad.be.
[428] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Vijfde Activiteitenverslag 2006, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 55.

bieden aan de arrondissementele diensten. De dossiers worden op dit punt ofwel behandeld door de lokale politie, ofwel door de arrondissementele diensten van de federale gerechtelijke politie, waarbij de centrale diensten in steun komen. Er zijn echter uitzonderingen op dit principe, welke zich situeren binnen de directie financieel-economische misdrijven. Meer concreet worden er tussen de federale politie en de Federal Computer Crime Unit afspraken gemaakt omtrent de samenwerking bij aanvallen op grote kritieke systemen. Als de federaal procureur beslist dat een dossier wordt behandeld door het federaal parket, wanneer de zaak m.a.w. wordt gefederaliseerd, dan kan de federaal procureur de FCCU aanduiden als opsporende eenheid. In dit geval draait de FCCU dan wel een autonoom dossier, wat een uitzondering uitmaakt op het wetgevend model. In de andere gevallen, biedt de FCCU haar diensten aan vanuit een ondersteunende rol.[429]

266. De grootste hindernis die de FCCU ondervindt gedurende het opsporen van cybercriminaliteit is het internationaal aspect van cybercrime. Volgens Luc Beirens zijn er van de 100 zaken die de FCCU behandelt, zeker 95 waarbij de landsgrenzen dienen te worden overgestoken. Gezien cybercrime zich in de meeste gevallen over de landsgrenzen heen manifesteert, zijn rechtshulpverzoeken een vaak gebruikt instrument door de FCCU. Hiernaast wordt bij internationale samenwerking ook op regelmatige basis gebruik gemaakt van instrumenten zoals de rogatoire commissies. Meer recent zijn er eveneens initiatieven met betrekking tot joint-investigation teams, waarbij informatie relatief vlot kan uitgewisseld worden van het ene dossier naar het andere. Het nadeel van de eerder genoemde rechtshulpverzoeken, zit hem in het feit dat deze grote vertragingen impliceren voor de afhandeling van het dossier. De uitwisseling met collega's verloopt in dit kader niet bijster vlot. In hoogdringende zaken, daarentegen, wordt de snelheid opgevoerd. In dit geval kan de FCCU zich wenden tot een 24u permanentiepunt, waardoor er op een relatief kort tijdsbestek een dossier kan opgestart en behandeld worden.[430]

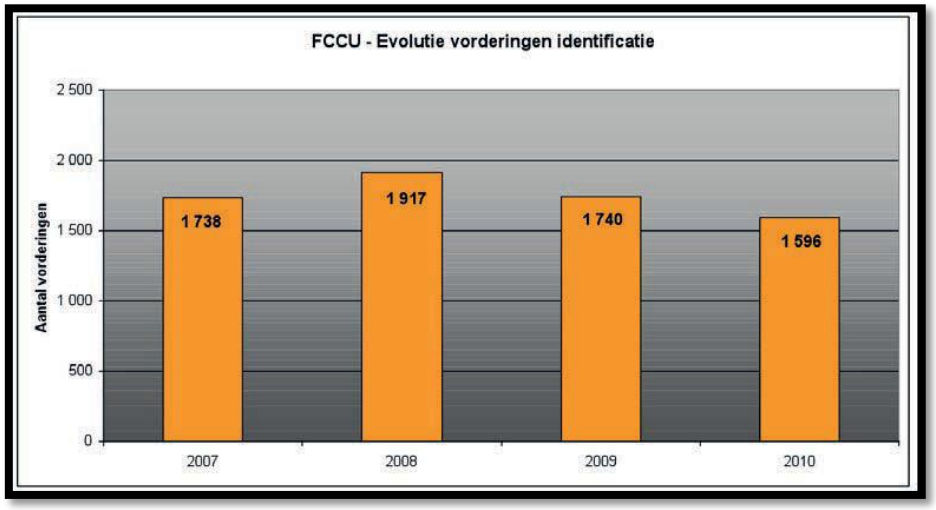
2.3.8 Enkele resultaten

267. Volgens het laatst gepubliceerde jaarverslag van de federale gerechtelijke politie, directie economische en financiële criminaliteit, heeft de FCCU gedurende het jaar 2010, 1.596 vorderingen ontvangen tot identificatie van internetgebruikers, zoals te zien valt in

[429] Zie bijlage 'interview met Luc Beirens'.
[430] Zie bijlage 'interview met Luc Beirens'.

onderstaande figuur.[431] Het betreft dan voornamelijk vorderingen tot identificatie van e-mailadressen, IP-adressen en pseudoniemen. Het aantal zit in een dalende tendens, te wijten aan een minder aantal vragen in het kader van grootschalige, internationale dossiers. Microsoft MSN is de koploper wat betreft het aantal uitgevoerde vorderingen, gevolgd door Google, eBay en Facebook.[432]

FIGUUR 6: DE EVOLUTIE VAN DE VORDERINGEN TOT IDENTIFICATIE VAN INTERNETGEBRUIKERS[433]



268. Met betrekking tot het meldpunt eCops zijn er eveneens cijfers vrijgegeven. De meldingen van inbreuken op economische wetgeving worden toegezonden aan de FOD Economie. Sinds augustus 2009 worden meldingen omtrent kinderpornografie en zedendelicten rechtstreeks overgemaakt aan de centrale dienst DJP/Mensenhandel van de Directie criminaliteit tegen personen van de federale politie.[434] Onderstaande tabel geeft het aantal ontvangen meldingen weer, evenals aan welke dienst deze werden toegewezen.

[431] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 25.
[432] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 25.
[433] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 25.
[434] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 25.

FIGUUR 7: AANTAL ONTVANGEN MELDINGEN VIA ECOPS[435]

FCCU - eCops: aantal meldingen en dispatching	2008	2009	2010
Totaal aantal meldingen te verwerken door FOD Economie	1.928	1.715	1.582
Aantal meldingen te verwerken door DJP/mensenhandel		2.939	3.078
Aantal meldingen te verwerken door FCCU		11.753	13.751
Aantal meldingen te verwerken door de Federale politie	12.534	14.692	16.829
Totaal aantal via webmelding op eCops	**14.462**	**16.407**	**18.411**

269. Onderstaande tabel geeft een indicatie van het soort misdrijven, waarop de klachten die via het aanmeldpunt eCops binnenkomen, betrekking hebben. De meldingen die via eCops ontvangen worden hebben juridisch gezien echter geen draagwijdte als klacht. In deze gevallen zal het slachtoffer, naast de melding via eCops, klacht moeten indienen bij de lokale politie, welke deze in een proces-verbaal kan gieten.[436]

FIGUUR 8: AARD VAN DE MISDRIJVEN ONTVANGEN VIA ECOPS[437]

FCCU - eCops: Informatie met betrekking tot misdrijven	2008	2009	2010
ICT-crime	616	554	839
Internetoplichting	6.741	8.082	7.669
Andere	1.596	1.255	1.979
Meldingen verwerkt door FCCU met relevante informatie inzake misdrijven	8.953	9.891	10.487
Percentage ten aanzien van het aantal verwerkte meldingen	71%	84%	76%

2.3.9 De FCCU op de weegschaal

270. De vraag die zich in dit kader stelt is of de FCCU zich kan meten met buitenlandse Computer Crime Units. Het antwoord op deze vraag hangt in grote mate af van welk land men als maatstaaf gebruikt. In vergelijking met het ene land excelleert de FCCU immers, terwijl de vergelijking met andere landen nauwelijks opgaat.[438] Luc Beirens stelt in eerste instantie dat, wat kennis en kunde betreft, de FCCU zich kan meten met eender welke buitenlandse

[435] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 26.
[436] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 25.
[437] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 26.
[438] Zie bijlage 'interview met Luc Beirens'.

Computer Crime Unit. Qua wettelijk kader, operationele personeelsbezetting, infrastructuur en middelen, is dit echter minder evident.[439]

271. Nederland is in dit kader een absolute topper, omwille van uiteenlopende redenen. Alleen al wat de vorming betreft, steekt Nederland er met kop en schouders bovenuit. Het land investeert immense bedragen in de vorming van de lokale recherche. Die lokale recherche vormt de basis, zij komen als eerste in contact met de veruitwendigingsvormen van cybercriminaliteit. Het is dan ook noodzakelijk om de mensen van de lokale politie te scholen, iets wat men in Nederland goed begrepen heeft. In Nederland gebeurt de scholing via online cursussen, opgesteld door private firma's. In België, daarentegen, geschiedt deze scholing volledig intern, wat op lange termijn niet houdbaar is. In Nederland is men daarenboven op een creatieve wijze bezig met de bestrijding van cybercriminaliteit. Zij zetten onderzoek op naar de wijze waarop men op een effectieve manier de structuren die cybercriminelen gebruiken, kan aanpakken. In Luxemburg en het Verenigd Koninkrijk lopen soortgelijke projecten. België loopt wat dat betreft hopeloos achter. In Nederland heeft men tevens een forensisch laboratorium opgericht, waar een team voor digitale expertise is in geïntegreerd. Dit team richt zich op moeilijke gevallen van datarecuperatie e.d.. Een soortgelijke instelling bestaat in België niet. Ons land heeft met het CERT wel stappen in die richting gezet. In die zin dat deze instantie instaat voor de melding van problemen waarvoor de gebruiker niet onmiddellijk naar de politie wil stappen. Nederland heeft eveneens een soortgelijke dienst, die geïntegreerd is in het National Cyber Security Centre. De instelling van de Nederlanders telt negentig personeelsleden, wat een groot aantal is, waar het CERT slecht zeven man sterk is. Uiteindelijk kan men stellen dat alles neerkomt op twee factoren: budget en de keuze van prioriteiten. Nederland heeft de afgelopen jaren van cybercriminaliteit een absolute prioriteit gemaakt. De capaciteiten van hun politiediensten wordt daar dan ook op toegespitst, wat leidt tot mooie resultaten. In België bestaat de tendens om alles te willen vervolgen en bestraffen. Dit is op zich een nobel doel, maar gezien de beperkte middelen en personeelsbestanden is dit niet echt houdbaar. In België wordt de capaciteit dan ook als dusdanig verspreid, waardoor je het risico loopt dat men weinig echt grondig kan doen.[440]

272. De Verenigde Staten stellen eveneens een veel groter budget ter beschikking. Op zich is dat niet onlogisch, de VS is een veel groter land dan België. Het geeft bijgevolg wel aan in

[439] Zie bijlage 'interview met Luc Beirens'.
[440] Zie bijlage 'interview met Luc Beirens'.

welke mate de Amerikaanse overheid zich bewust is van de schade die cybercriminaliteit aanricht. Dit weerspiegelt zich in het feit dat er in de VS een Cyber-Security Coördinator bestaat, Howard Schmidt, die deel uitmaakt van het kabinet van Barack Obama. In België bestaat deze functie niet. Het zou echter niet slecht zijn moest er in België, op het federale niveau binnen de regering, een soortgelijke functie in het leven worden geroepen.[441]

273. Ook in het Verenigd Koninkrijk lijkt men zich terdege bewust van de problematiek van cybercriminaliteit. Dit blijkt uit het feit dat de UK, tijdens de crisis van 2008, zowat op elk beleidsdomein heeft bespaard, behalve op de aanpak van cybercriminaliteit. Integendeel, er werd een budget van zeshonderd miljoen pond[442] vrijgemaakt, door de verkoop van enkele oorlogsfregatten.[443]

274. Niettemin doet de FCCU het lang niet slecht, zeker als men de beperkte personeelscapaciteit en budgetten in het achterhoofd houdt. Een land als Ierland staat er vele malen slechter voor, daar wordt de plaatselijke Cybercrime Unit bemand door twaalf personen.[444]

3. KRITISCHE BESCHOUWINGEN

275. De FCCU speelt een sleutelrol in de opsporing van cybercriminaliteit. Bij het uitoefenen van deze bevoegdheid wordt de FCCU geconfronteerd met tal van problemen. Deze problemen zijn deels te wijten aan de eigenheid van cybercriminaliteit zelf, deels aan de manier waarop de Belgische overheid tegen cybercriminaliteit aankijkt.

3.1 Het wettelijk kader

276. Vooreerst dient opgemerkt te worden dat het Belgisch wetgevend kader voldoende slagkracht geeft aan de FCCU om cybercrime aan te pakken. De materiële strafbaarstellingen en het strafprocesrecht staan grotendeels op punt, aldus Luc Beirens. Toch is er in het kader van de opsporing nog ruimte voor verbetering. Luc Beirens stelt dat vooral de BOM-wet, met

[441] Zie bijlage 'interview met Luc Beirens'.
[442] Omgerekend 740.623.485 euro.
[443] Zie bijlage 'interview met Luc Beirens'.
[444] Zie bijlage 'interview met Luc Beirens'.

haar stringente regeling, de mogelijkheden van de FCCU enigszins beperkt.[445] Om tot bijzondere opsporingsmethodes over te kunnen gaan is er een verantwoording vereist. In zekere zin moet de FCCU reeds op dat moment al aanwijzingen of elementen hebben, waardoor ze een bijzondere opsporingsmethode kan rechtvaardigen. Dit is echter niet altijd voor de hand liggend. Zo kan de FCCU op chatkanalen meelezen, maar zelf iets typen is niet toegestaan, want dat wordt beschouwd als zijnde een infiltratie. De FCCU mag evenmin proberen misdadigers in de val te lokken, gezien dit uitlokking uitmaakt, wat verboden is. In dat opzicht is de FCCU wat gekortwiekt, gezien ze steeds machtigingen van de onderzoeksrechter dienen af te wachten. In dit kader pleit Luc Beirens dan ook voor een versoepeling van de BOM-wet.[446]

3.2 Het verdere verloop na de opsporing

277. Een ander aspect waar vragen bij kunnen gesteld worden is in welke mate een opsporing ook effectief leidt tot de vervolging van de criminelen. Wanneer er zich zaken voordoen die zich van begin tot einde op Belgisch grondgebied afspelen, leidt de opsporing vaak tot de vervolging van de daders. In de meeste gevallen zijn er echter sporen naar het buitenland, wat de hele zaak bemoeilijkt. Niettemin heeft de FCCU successen geboekt in dit kader, al is dit niet steeds duidelijk en zichtbaar als resultaat voor de Belgische justitie. Zo heeft de FCCU een groot aantal dossiers behandeld omtrent e-banking fraude, waarbij er sporen naar het buitenland liepen. De FCCU heeft de daders kunnen identificeren, en zowel witwassers als hackers kunnen laten oppakken, waarna deze vervolgd werden. Toch is er lang niet altijd sprake van een succesvolle afloop.[447] Wanneer de FCCU haar dossier overdraagt aan de buitenlandse politiedienst in kwestie, kan de FCCU enkel hopen dat het dossier daar verder wordt afgehandeld. Dat is echter niet altijd het geval. Luc Beirens stelt in dit kader ook dat de mensen van de FCCU bij wijlen de indruk hebben dat een zaak in het buitenland eerder wordt tegengehouden, dan dat er effectief vooruitgang wordt geboekt.[448]

[445] Zie bijlage ‘interview met Luc Beirens’.
[446] Zie bijlage ‘interview met Luc Beirens’.
[447] Zie bijlage ‘interview met Luc Beirens’.
[448] Zie bijlage ‘interview met Luc Beirens’.

3.3 Het publieke bewustzijn

278. Een andere, toch wel markante vaststelling, is dat cybercriminaliteit nog steeds niet wordt beschouwd als zijnde een reëel, schadelijk probleem. Niemand, buiten de leden van de FCCU, lijkt de ernst van de situatie correct, en naar waarde in te schatten. Een treffend voorbeeld van deze stelling zien we in het defacement van websites.[449] Dit was enkele jaren geleden een prioriteit voor de FCCU. De FCCU bracht overheidsdiensten en belangrijke organisaties op de hoogte wanneer hun website gehacked was. Deze leken daar echter weinig belangstelling voor te tonen. In eerste instantie werd er door de diensten verrast gereageerd, maar toch werd er geen actie ondernomen. Het gevolg is dan ook dat nog geen week later, hun websites opnieuw werden gehacked. Niet alleen is dit schadelijk voor de desbetreffende overheidsdiensten en organisaties, daarenboven is het enorm frustrerend voor de personeelsleden van de FCCU. Het is dan ook geen overbodige luxe om werk te maken van meer bewustwording omtrent cybercriminaliteit bij het grote publiek. Idealiter zou eenieder een stuk verantwoordelijkheid moeten dragen. Een groot deel van de successen die cybercriminelen boeken zijn immers te wijten aan het feit dat de particuliere eindgebruikers zich onvoldoende wapenen tegen het fenomeen. Luc Beirens is dan ook de mening toegedaan dat het geen slechte zaak zou zijn om een deel van de verantwoordelijkheid te leggen bij de eindgebruiker.[450]

3.4 Bemerking omtrent het personeel en het budget

279. Op dit moment stelt de FCCU vijfendertig personen tewerk, waarvan er tien administratieve taken verrichten. Bij de RCCU's werken in totaal honderdzeventig mensen, waarvan er twintig administratief personeel zijn. In totaal zijn er dus honderdvijfenzeventig operationele personeelsleden, een laag aantal. Dat de Computer Crime Units in ons land met personeelsproblemen kampen is een publiek geheim, dat al vele jaren aansleept. Reeds in 2006 werd door de toenmalige regering vooropgesteld dat er in 2011 een totaal van tweehonderddrieënnegentig personen dienden tewerkgesteld te worden, binnen de FCCU en de RCCU's. Dat aantal is nooit gehaald. Het meest markante is echter dat de berekening van 2006 gestoeld is op de behoeften die er destijds waren. In 2012 ziet de wereld er echter

[449] Een defacement van een website is een aanval gepleegd door hackers, waardoor het uiterlijk van een website verandert.
[450] Zie bijlage 'interview met Luc Beirens'.

volkomen anders uit, waardoor de vooropgestelde cijfers uit 2006 ook al lang niet meer voldoen.[451]

280. Het gebrek aan personeel kent voornamelijk twee oorzaken. Ten eerste leent het budget van de FCCU en de RCCU's zich überhaupt niet tot een significante uitbreiding van het personeelskader. In 2010 werd er in totaal een budget van ruim 700.000 euro vrijgemaakt voor de Computer Crime Units. Op zich lijkt dit verre van een onaardig bedrag, maar schijn bedriegt echter. In vergelijkingen met de investeringen die in Nederland en het Verenigd Koninkrijk worden gemaakt, is dit een peulschil. De investering was daarenboven gericht op de aankoop en de vernieuwing van materiaal, niet zozeer op de financiering van bijkomend personeel. Ten tweede lijken veel informatici een job in de privé sector te verkiezen boven een carrière bij de politie. Informatici zijn heden ten dage gegeerd wild op de arbeidsmarkt. De privé sector kan vaak meer inspanningen doen om deze personen aan te werven, dan de overheid. De privé sector is dan ook vaak voordeliger voor informatici, niet alleen qua loon, maar ook qua extralegale voordelen, werkuren e.d..[452]

281. Ook wat de scholing van personeelsleden betreft is er nog werk aan de winkel. In dit kader kunnen we een voorbeeld nemen aan Nederland, dat door middel van online cursussen de politiediensten schoolt, beginnende vanaf het niveau van de lokale politie. In België gebeurt de scholing vooral binnen de eigen diensten, gezien er geen budget is voor het opstellen van een model zoals in Nederland.[453]

3.5 Gebrek aan een Koninklijk Besluit inzake dataretentie

282. Een belangrijke hiaat in onze wetgeving is een Koninklijk Besluit inzake dataretentie, ter uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Dit artikel stipuleert dat de Koning aan de hand van een Koninklijk Besluit de voorwaarden dient vast te leggen waaronder operatoren verkeersgegevens en identificatiegegevens van eindgebruikers dienen te bewaren. Er zou een bewaringstermijn van minimum twaalf maanden worden opgelegd. Dit Koninklijk Besluit heeft echter tot op

[451] Zie bijlage 'interview met Luc Beirens'.
[452] Zie bijlage 'interview met Luc Beirens'.
[453] Zie bijlage 'interview met Luc Beirens'.

vandaag het levenslicht nog niet gezien. Dit valt te betreuren, gezien dit de opsporende instanties de nodige hulp zou kunnen verschaffen.[454]

3.6 De hoeveelheid aangiftes

283. Een ander opmerkelijk gegeven is het aantal aangiftes van cybercriminaliteit. In 2010 kwamen er, via eCops, zo'n 18.411 meldingen binnen.[455] Symantec stelt in zijn jaarlijks cybercrime rapport dat er jaarlijks ruim 1,4 miljoen Belgen slachtoffer worden van cybercriminaliteit.[456] Wat dat laatste cijfer betreft dient men er wel rekening mee te houden dat Symatec een ontwikkelaar van beveiligingssoftware is, en de kans dus bestaat dat deze cijfers enigszins licht overdreven zijn. Niettemin staat het als een paal boven water dat er meer inbreuken plaatsvinden, dan diegene die effectief worden aangegeven. Men kan zich afvragen waarom er dergelijke discrepantie is tussen het aantal aangiftes en de hoeveelheid slachtoffers. Deze lage aangiftebereidheid kan zijn oorsprong vinden in allerlei redenen:[457]

- de slachtoffers veronderstellen dat aangifte doen geen zoden aan de dijk brengt;
- de slachtoffers ervaren de inbreuken niet als criminaliteit;
- de slachtoffers verzwijgen het liever, uit vrees dat hun goede naam schade zou oplopen. Dit heeft dan eerder betrekking op grote instellingen, zoals banken e.d.;
- de slachtoffers beseffen niet dat ze slachtoffer zijn geworden van cybercriminaliteit.

Hoofdstuk 5: De vervolging van cybercriminaliteit in België

1. INLEIDING

284. In dit hoofdstuk zal de vervolging van cybercriminaliteit besproken worden. In het Belgische rechtsbestel ligt de vervolging in handen van het Openbaar Ministerie, dat op grond

[454] Zie randnummers 210 e.v. voor een uitgebreide bespreking omtrent de problematiek van de dataretentie.
[455] Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php, 26.
[456] M. VAN DER VEN, "Cybercriminaliteit maakt 3 Belgische slachtoffers per minuut", *De Tijd*, 26 september 2011, www.tijd.be.
[457] Zie bijlage 'interview met Luc Beirens'.

van artikel 1 VTSv. het monopolie van de strafvordering heeft.[458] Algemeen gesteld, maakt de beslissing van het Openbaar Ministerie, om al dan niet te vervolgen, deel uit van een beleidskwestie. In de praktijk dient men aldus na te gaan welke misdrijven men wil vervolgen, en welke niet. Initieel gold, bij het opstellen van het Wetboek van Strafvordering, het principe dat elk misdrijf door het Openbaar Ministerie moest worden vervolgd.[459] Dit principe was echter niet werkbaar, en was al snel achterhaald. De algemene richtlijnen betreffende het strafrechtelijk beleid worden opgesteld door de minister van Justitie, welke de krijtlijnen bepalen waarbinnen vervolgingen dienen te worden ingesteld.[460] Nadien worden deze richtlijnen, op grond van artikel 143ter Ger. W., door het college van Procureurs-generaal verder uitgewerkt, in de vorm van omzendbrieven. [461] Deze ministeriële richtlijnen, en de omzendbrieven van het college van Procureurs-generaal in het bijzonder, zijn zeer belangrijke documenten. Zij pogen met name enerzijds, een uniform vervolgingsbeleid te bewerkstelligen en, anderzijds, aan prioriteitsstelling te doen.[462]

285. In het kader van de aanpak van cybercriminaliteit, zijn deze omzendbrieven van het college van Procureurs-generaal van aanzienlijk belang gebleken. In het volgende punt zal dan ook aan deze omzendbrieven de nodige aandacht worden besteed.

[458] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 2009, 749.
[459] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 2009, 753.
[460] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 2009, 754.
[461] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 2009, 754.
[462] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 2009, 754.

2. OMZENDBRIEVEN VAN HET COLLEGE VAN PROCUREURS-GENERAAL

2.1 Omzendbrieven met betrekking tot de aanpak van verschijningsvormen van cybercriminaliteit

2.1.1 Omzendbrief COL 13 van 1 oktober 1998

286. De eerste omzendbrief van het college van Procureurs-generaal die betrekking heeft op de thematiek van dit werk, is die van 1 oktober 1998.[463] Deze omzendbrief kwam er naar aanleiding van de wijziging van de wet van 30 juni 1994, door de wet van 10 juni 1998.[464] De wetswijziging voegde het nieuw artikel 46bis, toe aan het Wetboek van Strafvordering. Verder werden de artikelen 88bis, 90quater §2, 90sexies en septies van het Wetboek van Strafvordering gewijzigd, evenals artikel 109ter E §2. Tenslotte werd artikel 90ter §2 Sv. uitgebreid.[465] De omzendbrief bestaat, met inbegrip van enkele kleine verduidelijkingen, quasi volledig uit een artikelsgewijze commentaar bij de nieuwe bepalingen. Echte krachtlijnen voor de concrete toepassing van de bepalingen worden er echter niet uitgezet.

2.1.2 Omzendbrief COL 12 van 3 juni 1999

287. In tegenstelling tot voorgaande omzendbrief, bevat deze wel degelijk concrete richtlijnen omtrent het opsporings- en vervolgingsbeleid. Deze omzendbrief heeft de bestrijding van mensenhandel en kinderpornografie tot doel.[466] De richtlijn strekt ertoe een coherent opsporings- en vervolgingsbeleid uit te werken in de strijd tegen laatstgenoemde misdrijven. Meer bepaald wordt er gehamerd op de coördinatie van de opsporingen en de vervolgingen, waarbij een belangrijke rol is weggelegd voor de verbindingsmagistraten, zowel op het niveau van het parket-generaal, als op het niveau van de parketten van eerste

[463] Omzendbrief van het college van Procureurs-generaal 1 oktober 1998 betreffende de wet van 10 juni 1998 tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en –telecommunicatie, nr. COL 13/98, www.om-mp.be/extern/getfile.php?p_name=3319355.PDF.

[464] Wet 10 juni 1998 tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en -telecommunicatie, *B.S.* 22 september 1998.

[465] Omzendbrief van het college van Procureurs-generaal 1 oktober 1998 betreffende de wet van 10 juni 1998 tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en –telecommunicatie, nr. COL 13/98,www.om-mp.be/extern/getfile.php?p_name=3319355.PDF.

[466] Omzendbrief van het College van Procureurs-generaal 3 juni 1999, betreffende de Ministeriële richtlijn houdende het opsporings- en vervolgingsbeleid betreffende mensenhandel en kinderpornografie, nr. COL 12/99, www.om-mp.be/extern/getfile.php?p_name=3318569.PDF.

aanleg. De kernpunten in dit kader zijn dat de verbindingsmagistraat dient op te treden als aanspreekpunt, moet instaan voor de follow-up van dossiers, een jaarverslag dient op te maken en inlichtingen dient te verzamelen en uit te wisselen met de verschillende diensten van het parket. Zij dienen daarenboven de procureur-generaal op de hoogte te houden van belangrijke dossiers. De omzendbrief bepaalt daarenboven enkele prioriteiten aangaande de opsporing en vervolging, evenals een concrete weergave van de organisatie van de opsporingen.[467] Aldus dient er gewezen te worden op het feit dat de opsporingsdiensten en de vervolgende instanties verplicht zijn rekening te houden met deze omzendbrief, in de gevallen waarbij kinderporno in een informaticacontext het voorwerp uitmaakt van een onderzoek.

288. Tenslotte dient nog vermeld te worden dat deze omzendbrief werd aangepast door de omzendbrief van 30 april 2004. [468] Gezien de omzendbrief in kwestie enkel betrekking heeft op mensenhandel, en niet op kinderpornografie, zal deze niet nader behandeld worden.

2.1.3 Omzendbrief COL 1 van 14 februari 2002

289. Deze omzendbrief kwam er naar aanleiding van de inwerkingtreding van de nieuwe wet van 28 november 2000 inzake informaticacriminaliteit. [469] De omzendbrief bevat een uitgebreide inhoudelijke bespreking van de wet, met aandacht voor de aanpassingen van het materiële strafrecht en het strafprocesrecht. Wat belangrijker is voor het opsporings- en vervolgingsbeleid an sich, is dat de omzendbrief zes nieuwe parketcodes boven de doopvont houdt:[470]

- valsheid in informatica - code 21C;
- informaticabedrog - code 20J;
- ongeoorloofde toegang tot een informaticasysteem - code 20K;
- data- en informaticasabotage - code 20L;

[467] Omzendbrief van het College van Procureurs-generaal 3 juni 1999, betreffende de Ministeriële richtlijn houdende het opsporings- en vervolgingsbeleid betreffende mensenhandel en kinderpornografie, nr. COL 12/99, www.om-mp.be/extern/getfile.php?p_name=3318569.PDF.
[468] Omzendbrief van het college van Procureurs-generaal 30 april 2004 betreffende het opsporings- en vervolgingsbeleid betreffende mensenhandel – Aanpassing van de richtlijn van de minister van Justitie, nr. COL 10/2004, www.om-mp.be/extern/getfile.php?p_name=3447098.PDF.
[469] Omzendbrief van het college van Procureurs-generaal 14 februari 2002 betreffende de wet inzake informaticacriminaliteit, nr. COL 1/2002, www.om-mp.be/omzendbrief/4017270/omzendbrieven_2002.html.
[470] Omzendbrief van het college van Procureurs-generaal 14 februari 2002 betreffende de wet inzake informaticacriminaliteit, nr. COL 1/2002, www.om-mp.be/omzendbrief/4017270/omzendbrieven_2002.html.

- weigering tot het verlenen van de door de onderzoeksrechter gevorderde medewerking (in het kader van een zoeking in het informaticasysteem of hinderen van een door de onderzoeksrechter bevolen zoeking in het informaticasysteem - code 20M;
- weigering tot het verlenen van de door de onderzoeksrechter gevorderde medewerking (in het kader van telecommunicatie) - code 20N.

290. De toepassing van deze codes werd vooropgesteld om een adequate statische verwerking van gegevens te kunnen nastreven.

291. Tijdens de parlementaire voorbereidingen van de wet van 28 november 2000 bleek dat er een noodzaak bestond tot evaluatie van de toepassing van de nieuwe wet. De omzendbrief bevat in dit opzicht dan ook bepalingen omtrent deze kwalitatieve evaluatie. Meer bepaald stelt men voorop dat er gegevens dienen verzameld te worden, waardoor de juridische en operationele effectiviteit van de wet kan worden nagegaan. De Omzendbrief COL 16/2004 werkt in dit kader nadere regels uit.[471]

2.1.4 Omzendbrief COL 8 van 9 april 2004

292. Deze omzendbrief heeft de wet van 7 mei 1999 op de kansspelen, de kansspelinrichtingen en de bescherming van de spelers als voorwerp.[472] [473] Op grond van deze wet geldt er een verbod om spelen, die aan de kenmerken van een kansspel beantwoorden, via het internet, sms of digitale televisie aan te bieden. Naast een artikelsgewijze bespreking van de wet, bepaalt de omzendbrief eveneens de prioriteiten van het strafrechtelijk beleid in dit kader. Meer bepaald wordt uitgewerkt welke politiediensten bevoegd zijn voor deze materie, en op welke manier zij deze bevoegdheden op een adequate wijze dienen uit te oefenen.[474] In

[471] Omzendbrief van het college van Procureurs-generaal betreffende de wet inzake de informaticacriminaliteit - Addendum aan de §§ 58 en 59 van de omzendbrief nr. COL 1/2002, nr. COL 16/2004, www.om-mp.be/omzendbrief/4016876/omzendbrieven_2004.html.
[472] Omzendbrief van het college van Procureurs-generaal 9 april 2004 betreffende de wet van 7 mei 1999 op de kansspelen, de kansspelinrichtingen en de bescherming van de spelers, nr. COL 8/2004, www.om-mp.be/omzendbrief/4016876/omzendbrieven_2004.html.
[473] Wet 7 mei 1999 op de kansspelen, de kansspelinrichtingen en de bescherming van de spelers, *B.S.* 3 december 1999.
[474] Omzendbrief van het college van Procureurs-generaal 9 april 2004 betreffende de wet van 7 mei 1999 op de kansspelen, de kansspelinrichtingen en de bescherming van de spelers, nr. COL 8/2004, www.om-mp.be/omzendbrief/4016876/omzendbrieven_2004.html.

dit kader is ook Omzendbrief COL 2/2006 van aanzienlijk belang.[475] Deze omzendbrief bevat eveneens bepalingen omtrent de kansspelen, met de nadruk op de aanpak van clandestiene inrichtingen. De omzendbrief bevat richtlijnen voor de opsporingsdiensten omtrent de opsporing ten huize, en de huiszoeking in clandestiene inrichtingen. Verder wordt er bepaald wat er dient te gebeuren met de materiële inrichting en de opbrengsten van de clandestiene goktenten.[476]

2.1.5 Omzendbrief COL 6 van 21 maart 2006

293. Deze omzendbrief is gericht op de aanpak van racisme en xenofobie.[477] De omzendbrief stelt een eenvormige werkwijze voorop in de aanpak van deze misdrijven, zowel voor de opsporings- en de vervolgingsdiensten. Het gaat in dit kader meer om praktische richtlijnen, zoals de te gebruiken parketcodes, en op welke manier de politie en het parket gevallen van racisme en xenofobie dienen te verwoorden in een proces-verbaal.[478]

2.1.6 Omzendbrief COL 2 van 19 februari 2009

294. De omzendbrief van 19 februari 2009 is gericht op de aanpak van namaak en piraterij van intellectuele eigendomsrechten.[479] Vooral dit tweede aspect is, in het kader van dit werk, van belang. De omzendbrief geeft een artikelsgewijze commentaar bij de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten.[480] De omzendbrief bevat tevens bepalingen omtrent de opsporing en de vaststelling van de inbreuken, evenals een omschrijving van de specifieke

[475] Omzendbrief van het college van Procureurs-generaal 24 februari 2006 betreffende de kansspelen en de clandestiene inrichtingen, nr. COL 2/2006, www.om-mp.be/omzendbrief/4017068/omzendbrieven_2006.html.
[476] Omzendbrief van het college van Procureurs-generaal 24 februari 2006 betreffende de kansspelen en de clandestiene inrichtingen, nr. COL 2/2006, www.om-mp.be/omzendbrief/4017068/omzendbrieven_2006.html.
[477] Omzendbrief van het college van Procureurs-generaal 21 maart 2006 betreffende racisme en xenofobie, nr. COL 6/2006, www.om-mp.be/omzendbrief/4017068/omzendbrieven_2006.html.
[478] Omzendbrief van het college van Procureurs-generaal 21 maart 2006 betreffende racisme en xenofobie, nr. COL 6/2006, www.om-mp.be/omzendbrief/4017068/omzendbrieven_2006.html.
[479] Wet 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten, *B.S.* 18 juli 2007.
[480] Omzendbrief van het college van Procureurs-generaal 19 februari 2009 betreffende de toepassing van de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten, nr. COL 2/2009, www.om-mp.be/omzendbrief/4123047/omzendbrieven_2009.html.

onderzoeksbevoegdheden. Verder worden er ook richtlijnen opgesteld omtrent de wijze waarop de vervolging dient te geschieden.[481]

295. Gezien de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten in 2010 werd gewijzigd[482], kwam er in dit kader ook een nieuwe omzendbrief tot stand.[483]

2.1.7 Omzendbrief COL 14 van 17 december 2009

296. Deze omzendbrief kwam er na het ontstaan van de Telecommunicatierichtlijn, en heeft betrekking op de medewerkingsverplichtingen zoals deze zijn beschreven in de artikelen 46bis §2, 88bis §2 en 90quater §2 Sv..[484] Deze omzendbrief kwam er na vaststellingen dat de politiediensten moeilijkheden ondervonden bij de uitvoering van de vorderingen beschreven in de voorafgaande artikelen van het Wetboek van Strafvordering. De operatoren stelden immers al te vaak dat de gevraagde informatie niet beschikbaar was, of dat er aanzienlijke wachttijden waren. De omzendbrief wil hier tegen optreden door de creatie van een uniform strafrechtelijk beleid in deze context. De omzendbrief bevat dan ook richtlijnen voor zowel de politiediensten als de parketten. Zo dienen de politiediensten bij een weigering tot medewerking van een operator, evenals bij laattijdige of gebrekkige medewerking, steeds een proces-verbaal op te maken. Wat betreft de parketten, stelt de omzendbrief dat het niet-meewerken van operatoren niet systematisch dient uit te monden in een dagvaarding, maar dat er wel een gepaste reactie dient te komen, afhankelijk van het specifieke geval.[485]

[481] Omzendbrief van het college van Procureurs-generaal 19 februari 2009 betreffende de toepassing van de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten, nr. COL 2/2009, www.om-mp.be/omzendbrief/4123047/omzendbrieven_2009.html.
[482] Wet 28 april 2010 houdende diverse bepalingen, *B.S.* 10 mei 2010.
[483] Omzendbrief van het college van Procureurs-generaal 31 december 2010 betreffende de wijzigingen die door de wet van 28 april 2010 houdende diverse bepalingen werden aangebracht aan de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten, nr. COL 23/2010, www.om-mp.be/omzendbrief/4124639/omzendbrieven_2010.html.
[484] Omzendbrief van het college van Procureurs-generaal 17 juli 2009 betreffende de Telecommunicatierichtlijn inzake het opsporings- en vervolgingsbeleid betreffende inbreuken op de medewerkingsverplichtingen vervat in de artikelen 46bis § 2, 88bis § 2 en 90quater § 2 van het wetboek van strafvordering, nr. COL 14/2009, www.om-mp.be/omzendbrief/4123047/omzendbrieven_2009.html.
[485] Omzendbrief van het college van Procureurs-generaal 17 juli 2009 betreffende de Telecommunicatierichtlijn inzake het opsporings- en vervolgingsbeleid betreffende inbreuken op de medewerkingsverplichtingen vervat in de artikelen 46bis § 2, 88bis § 2 en 90 quater § 2 van het wetboek van strafvordering, nr. COL 14/2009, www.om-mp.be/omzendbrief/4123047/omzendbrieven_2009.html.

2.2 Omzendbrieven met betrekking tot de internationale samenwerking

297. Het college van Procureurs-generaal heeft eveneens enkele omzendbrieven opgesteld omtrent de internationale samenwerking in strafzaken. Gezien cybercriminaliteit zich vaak grensoverschrijdend manifesteert, zijn deze omzendbrieven niet zonder belang. Gezien deze omzendbrieven steeds tot hoofddoel hebben om de moeilijkheden in het kader van internationale samenwerking weg te werken, zullen deze niet nader in detail worden besproken. De omzendbrieven die internationale samenwerking in strafzaken als voorwerp hebben zijn de volgende:[486]

- Omzendbrief COL 15/1999: gemeenschappelijke omzendbrief van de minister van Justitie en het college van Procureurs-generaal met betrekking tot de goede praktijken inzake internationale rechtshulp in strafzaken tussen de lidstaten van de Europese Unie;
- Omzendbrief COL 2/2000: gezamenlijke omzendbrief van de minister van Justitie en het college van Procureurs-generaal betreffende de internationale politiesamenwerking met een gerechtelijke finaliteit;
- Omzendbrief COL 15/2004: internationale samenwerking in strafzaken – Eurojust;
- Omzendbrief COL 5/2005: gemeenschappelijke omzendbrief van de minister van Justitie en het college van Procureurs-generaal betreffende de internationale rechtshulp in strafzaken;
- Omzendbrief COL 15/2005: gemeenschappelijke omzendbrief van de minister van Justitie en het college van Procureurs-generaal betreffende de EU-Overeenkomst inzake de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie;
- Omzendbrief COL 5/2006: gemeenschappelijke omzendbrief van de minister van Justitie en het college van Procureurs-generaal betreffende de internationale rechtshulp in strafzaken;
- Omzendbrief COL 21/2010: internationale samenwerking in strafzaken, Inventarisatie van de problematische internationale rogatoire commissies.

[486] www.om-mp.be/omzendbrieven.html

2.3 Omzendbrieven met betrekking tot de werking van de FCCU

298. Het college van Procureurs-generaal heeft eveneens enkele omzendbrieven uitgevaardigd, die van belang zijn voor de concrete werking van de FCCU.

2.3.1 Omzendbrief COL 2 van 7 maart 2002

299. De omzendbrief handelt over de taakverdeling, de samenwerking, de coördinatie en de integratie tussen de lokale en de federale politie inzake de opdrachten van gerechtelijke politie.[487] Deze omzendbrief is van belang omdat hij de krijtlijnen vaststelt omtrent de verdeling van de opdrachten tussen de lokale en federale politie. Meer concreet zorgt de omzendbrief dat de verschillende diensten de misdrijven behandelden die tot hun bevoegdheidssfeer behoren, wat ook zijn weerslag heeft op de werking van de Federal Computer Crime Unit.

2.3.2 Omzendbrief COL 9 van 18 juni 2009

300. Waar bovenstaande omzendbrief een meer algemene draagwijdte heeft, heeft de omzendbrief van 18 juni 2009 een meer specifiek toepassingskader.

301. Deze omzendbrief heeft met name betrekking op de samenwerkingsmodaliteiten tussen het federaal parket en de centrale directies, waaronder het DJF, waar de FCCU deel van uitmaakt. In de omzendbrief zijn er dan ook bepalingen terug te vinden omtrent de werking van de FCCU. Zo stelt de omzendbrief dat de FCCU kan gelast worden met het onderzoek, autonoom of ondersteunend, in de gevallen waarbij kritieke ICT-infrastructuur wordt bedreigd, of in het geval van een complex onderzoek. [488]

[487] Omzendbrief van het college van Procureurs-generaal 7 maart 2002 betreffende de regeling van de taakverdeling, de samenwerking, de coördinatie en de integratie tussen de lokale en de federale politie inzake de opdrachten van gerechtelijke politie, nr. COL 2/2002, www.om-mp.be/omzendbrief/4017270/omzendbrieven_2002.html.

[488] Omzendbrief van het college van Procureurs-generaal 18 juni 2009 als addendum aan de gemeenschappelijke omzendbrief van de minister van Justitie en het college van Procureurs-generaal 5/2002 betreffende het federaal parket - Modaliteiten van samenwerking tussen het federaal parket en de centrale directies van de algemene directie van de gerechtelijke politie van de federale politie, nr. COL 9/2009, www.om-mp.be/omzendbrief/4123047/omzendbrieven_2009.html.

3. STATISTISCHE GEGEVENS OMTRENT DE VERVOLGING

3.1 Inleiding

302. De vele omzendbrieven van het college van Procureurs-generaal omtrent de thematiek van cybercriminaliteit, wijst op een zeker bewustzijn over de omvang van het probleem. De vraag blijft echter in welke mate het Openbaar Ministerie cybercriminaliteit al dan niet vervolgt. Het antwoord op deze vraag is te vinden in de jaarstatistieken van het Openbaar Ministerie.[489] Deze jaarstatistieken bevatten, per burgerlijk jaar, informatie over de opsporing en vervolging van strafzaken door de correctionele parketten.

303. In dit punt zal nagegaan worden in welke mate parketten optreden tegen informaticamisdrijven. Meer bepaald zullen de cijfers met betrekking tot de instroom en de uitstroom worden besproken, evenals het aantal hangende zaken. De gegevens die u in onderstaande tabellen terug kan vinden hebben betrekking op de jaren 2007 tot 2010. Tevens zijn de gegevens van het jaar 2003 opgenomen, gezien dit toelaat om over een tijdsbestek van een klein decennium, duidelijke tendensen waar te nemen. De cijfers van 2010 zijn de meest recente statistieken die werden vrijgegeven door de statistische analisten van het Openbaar Ministerie.

304. Tenslotte dienen er omtrent deze cijfers nog enkele bemerkingen gemaakt te worden. Vooreerst hebben de resultaten enkel betrekking op specifieke informaticamisdrijven, waaronder diegene die door de wet inzake informaticacriminaliteit zijn ingevoerd. De a-specifieke informaticamisdrijven zijn niet vervat in het luik 'informatica'. Zo zijn bijvoorbeeld de verspreiding van kinderpornografie en de oplichting in een informaticacontext hier niet terug te vinden, zij vallen immers onder hun respectievelijke traditionele kwalificaties. Gezien in de jaarstatistieken bij laatstgenoemde kwalificaties geen onderscheid wordt gemaakt tussen het feit of deze al dan niet gepleegd zijn door middel van informaticasystemen, worden de cijfers hieromtrent niet verder besproken. Vervolgens dient erop gewezen te worden dat de cijfers betrekking hebben op de werking van de rechtbanken van eerste aanleg. Men mag het cijfermateriaal dus niet op een veralgemenende wijze

[489] www.om-mp.be/sa/start/n/home.html.

interpreteren. Niettemin scheppen de cijfers wel een beeld over de manier waarop de parketten de misdrijven in het kader van cybercriminaliteit benaderen.

3.2 Instroom van zaken met betrekking tot de tenlastelegging 'informatica'

305. De instroom is samengesteld uit alle zaken die het parket in de loop van het burgerlijke jaar heeft ontvangen. Het gaat in dit kader zowel om nieuwe, als om heropende zaken.[490]

FIGUUR 9: INSTROOM VAN ZAKEN BIJ DE PARKETTEN VAN EERSTE AANLEG WAT BETREFT DE TENLASTELEGGING 'INFORMATICA'

	2003	2007	2008	2009	2010
Informatica	1.034	7.831	9.867	12.631	17.346

306. In het jaar 2010 was er een instroom van 17.346 zaken omtrent informatica. Als we de evolutie op vier jaar tijd bekijken, van 2007 tot 2010, zien we een aanzienlijke stijging van het aantal zaken. Wanneer de cijfers van het jaar 2010 naast die van het jaar 2003 worden gelegd, is de stijging enorm te noemen. Op een periode van zeven jaar is het aantal zaken maar liefst verzeventienvoudigd.

307. Er zijn verschillende factoren die aan de grondslag zouden kunnen liggen van de forse stijging van het aantal zaken, die de verschillende parketten voor de kiezen krijgen. Een eerste mogelijke verklaring ligt in het feit dat cybercriminaliteit zich vanaf de eeuwwisseling steeds meer is beginnen te manifesteren. Dit wordt bevestigt door Luc Beirens. Laatstgenoemde stelt namelijk dat het aantal zaken sinds zijn aanstelling tot nu, in een snel tempo is toegenomen.[491] Gezien er meer gevallen zijn, krijgen de parketten er ook meer mee te maken. Een andere verklaring kan gevonden worden in het feit dat het grote publiek sneller aangifte doet van dergelijke feiten. Dit laatste wordt wel enigszins tegengesproken door diezelfde Luc Beirens. Naar zijn mening bestaat er wel degelijk een maatschappelijk bewustzijn omtrent cybercriminaliteit, maar niet in die aard dat dit zou leiden tot een wildgroei van het aantal aangiftes.[492] Een laatste reden kunnen we vinden bij de opsporingsdiensten zelf, die door bijkomende expertise en middelen, meer zaken kunnen opsporen.

[490] www.om-mp.be/sa/jstat2010/n/home.html.
[491] Zie bijlage 'interview met Luc Beirens'.
[492] Zie bijlage 'interview met Luc Beirens'.

3.3 Hangende zaken met betrekking tot de tenlastelegging 'informatica'

308. Deze zaken zijn zaken waarvoor het Openbaar Ministerie nog geen beslissing heeft genomen, die kan beschouwd worden als een beslissing die de zaak afsluit. Het betreft zaken waar op 1 januari van het respectievelijke jaar nog geen afsluitende beslissing is genomen.[493]

FIGUUR 10: HANGENDE ZAKEN BIJ DE PARKETTEN VAN EERSTE AANLEG WAT BETREFT DE TENLASTELEGGING 'INFORMATICA'

	2003	2007	2008	2009	2010
Informatica	214	1.635	2.360	2.980	3.291

309. Ook hier zien we, net als bij de instroom, een stijging van het aantal zaken. Het dient wel te worden opgemerkt dat de stijging lang niet zo significant is, als diegene die bij de instroom valt waar te nemen. Enerzijds, is deze stijging te wijten aan het feit dat de instroom aanzienlijk stijgt. Anderzijds, aan de discrepantie tussen de capaciteit van de opsporende instanties en die van de vervolgende instanties. Waar de FCCU zich van zijn taak dient te kwijten met 35 personen, zijn de parketten voorzien van een veel groter personeelsbestand.

3.4 Uitstroom van zaken met betrekking tot de tenlastelegging 'informatica'

310. De gegevens in onderstaande figuur hebben betrekking op de zaken die in de loop van het respectievelijke burgerlijk jaar zijn afgesloten. De beslissingen die een zaak afsluiten zijn de volgende:[494] [495]

- de zonder gevolgstellingen;
- de terbeschikkingstellingen;[496]
- de samenvoegingen;[497]
- de betaalde minnelijke schikkingen;

[493] www.om-mp.be/sa/jstat2010/n/home.html.
[494] www.om-mp.be/sa/jstat2010/n/home.html.
[495] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 2009, 755.
[496] Het betreft de zaken die werden overgemaakt aan andere instanties zoals het federaal parket of een parket van eerste aanleg in een ander rechtsgebied, waarna deze opnieuw worden samengevoegd.
[497] Krachtens art. 566 Ger. W. kunnen verschillende vorderingen die afzonderlijk werden ingesteld en voor verschillende rechtbanken zouden moeten worden gebracht, voor dezelfde rechtbank worden samengevoegd indien zij samenhangend zijn. Wanneer een zaak wordt samengevoegd in de moederzaak, worden alle beslissingen opgenomen in deze moederzaak. Aan de dochterzaak wordt de beslissing van de 'voeging' toegekend.

- de succesvol voltooide bemiddelingen in strafzaken;
- de rechtstreekse dagvaardingen;
- de vaststellingen voor de raadkamer voor de regeling van de rechtspleging.

FIGUUR 11: UITSTROOM VAN ZAKEN BIJ DE PARKETTEN VAN EERSTE AANLEG WAT BETREFT DE TENLASTELEGGING 'INFORMATICA'

	2003	2007	2008	2009	2010
Zonder gevolgstelling	495	4.155	5.463	7.499	10.861
Terbeschikkingstellingen	74	818	1.169	1.367	1.559
Samenvoegingen	212	2.012	2.239	3.161	3.679
De betaalde minnelijke schikkingen	1	7	0	10	15
Bemiddeling in SZ succesvol voltooid	1	7	19	21	22
Rechtstreekse dagvaarding	6	37	61	75	119
Vaststelling voor de raadkamer	14	67	71	74	95
Totaal aantal	803	7.831	9.122	12.207	16.170

311. Net zoals bij de instroom en het aantal hangende zaken, zien we ook hier weer een uitgesproken stijging van het aantal zaken. Dit is logisch, gezien de uitstroom een resultante is van de instroom, waardoor de stijgende tendens zich op algemene wijze manifesteert.

312. Wat het meest in het oog springt bij het bovenstaande cijfermateriaal, is het aantal geseponeerde zaken. De overgrote meerderheid van de behandelde zaken wordt door het Openbaar Ministerie zonder gevolg gesteld. Ook het aantal samenvoegingen is opmerkelijk te noemen. In een absoluut minimum van de gevallen wordt er overgaan tot een rechtstreekse dagvaarding. Ook minnelijke schikkingen komen amper voor. De reden waarom er in zo'n grote mate wordt geseponeerd ligt voor de hand. De bewijsvoering, die op de schouders van het Openbaar Ministerie rust, is in het kader van cybercriminaliteit niet zo vanzelfsprekend. Daders van cybercriminaliteit opsporen is één zaak, het effectief bewijs leveren een andere. Dit verklaart meteen ook het lage aantal minnelijke schikkingen en rechtstreekse dagvaardingen.

Hoofdstuk 6: De straftoemeting door de rechter

1. INLEIDING

313. In de voorafgaande hoofdstukken werd achtereenvolgend de opsporing en de vervolging behandeld. Meer bepaald werd er besproken op welke wijze de FCCU tewerk gaat in de strijd tegen cybercriminaliteit, evenals de aanpak van de parketten bij de rechtbanken van eerste aanleg. Zowel de opsporing, als de vervolging, worden gekenmerkt door een zekere mate van beleid, waarbij vanuit een centrale aansturing prioriteiten worden gesteld. In het kader van de straftoemeting is dit echter niet het geval, er is met name geen instantie die een soort van 'senceting guidelines' uitvaardigt.[498] De beoordelingsvrijheid van de rechter in het kader van de straftoemeting is één van de stokpaardjes van de rechterlijke macht. Deze beoordelingsvrijheid zag het levenslicht in de Code pénal van 1810, zij het zeer beperkt. Het Strafwetboek van 1867 voerde de verzachtende omstandigheden in, en met de Probatiewet van 1964 werd de rechter opnieuw een bijkomend instrument tot individualisering van de sancties aangereikt, in de vorm van de opschorting van de uitspraak.[499] Niettemin wordt de beoordelingsvrijheid van rechter ook beperkt. Zo is hij onderworpen aan de wettelijke motiveringsplicht, die in 1987 werd ingevoerd.[500] Daarenboven dient de rechter zich te schikken naar het vervolgingsbeleid, dat zal bepalen welk type van misdrijven, en welke personen uiteindelijk onderworpen worden aan de straftoemeting.

314. Tot het einde van de jaren '90 diende de rechter, in gevallen van cybercriminaliteit, zijn toevlucht te zoeken tot artikelen die initieel, in geen enkel opzicht, de bestraffing van zulke feiten voor ogen hadden. De kwaliteit van de rechtspraak die hieruit voortvloeide was dan ook navenant. In vele gevallen raakten de hersenspinsels van de rechters werkelijk kant nog wal. De eerder besproken 'Bistel'- en 'ReDaTtacK'-zaak zijn hiervan stille getuigen.

315. De wet van 28 november 2000 inzake informaticacriminaliteit heeft getracht deze scheve situatie recht te zetten. Met nieuwe strafbaarstellingen werd de rechter adequaat

[498] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 2009, 477.
[499] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 2009, 476-477.
[500] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 2009, 481.

instrumentarium aangereikt. De vraag in dit verband is dan ook of deze nieuwe instrumenten hebben geleid tot effectieve veroordelingen. Om na te gaan of de wet inzake informaticacriminaliteit zijn vruchten heeft afgeworpen, dient men zich, vanzelfsprekend, te wenden tot de jurisprudentie. Wat cybercriminaliteit betreft dienden we voorafgaand reeds vast te stellen dat het aantal geseponeerde zaken, het aantal effectieve dagvaardingen in ruime mate overstijgt. Dit heeft tot gevolg dat het aantal zaken omtrent cybercriminaliteit, die effectief voor een rechtbank komen, niet bepaald groot te noemen is. Niettemin zal in dit hoofdstuk worden nagegaan op welke wijze de wet van 28 november 2000 haar uitwerking heeft gevonden in de praktijk. De bespreking hiervan zal geschieden overeenkomstig de nieuwe strafbaarstellingen, zoals de wet inzake informaticacriminaliteit ze heeft ingevoerd.

2. BESPREKING VAN DE RELEVANTE RECHTSPRAAK

2.1 Vonnis van 15 december 2003 van de correctionele rechtbank te Eupen

316. Deze zaak is de eerste geweest waarbij een misdrijf werd beoordeeld volgens één van de bepalingen uit de wet inzake informaticacriminaliteit, met name artikel 550bis Sw.[501] In casu ging het om een man, die had geprobeerd om in te breken in de computersystemen van Euregio.net, een internetdienstenleverancier. De verdachte maakte hierbij gebruik van een programma, dat paswoorden genereerde, en deze paswoorden had proberen toe te passen op de website in kwestie. De pogingen van de verdachte waren echter zonder succes. De correctionele rechtbank achtte de man in kwestie schuldig aan de poging tot het misdrijf computerinbraak, zoals dat wordt beschreven in artikel 550bis Sw.[502]

2.2 Vonnis van 28 november 2005 van de correctionele rechtbank te Dendermonde

317. Op 28 november 2005 velde de correctionele rechtbank van Dendermonde een vonnis met betrekking tot artikel 210bis Sw..[503] Omtrent het feitenrelaas kunnen we kort zijn. Op 19 oktober 2004 legde E.V. bij de politie klacht neer wegens eerroof en valse naamdracht, omwille van het feit dat een andere persoon onder de naam van E.V. een hotmailaccount had

[501] Corr. Eupen 15 december 2003,www.internet-observatory.be, noot H. GRAUX.
[502] Corr. Eupen 15 december 2003, www.internet-observatory.be, noot H. GRAUX.
[503] Corr. Dendermonde 28 november 2005, *RABG* 2007, (427) 427.

aangemaakt, en vervolgens een e-mail had gestuurd naar een schepen. De RCCU van Dendermonde kwam erachter dat het IP-adres van de verzender van de e-mail aangesloten was bij Skynet. De verzender bleek een man te zijn, U.T. genaamd. De procureur des Konings vorderde, o.g.v. artikel 46bis Sv., de identificatie van de verzender bij Skynet. Nadien bekende de beklaagde bij zijn verhoor. De tenlastelegging in deze zaak betrof valsheid in informatica. De correctionele rechtbank van Dendermonde oordeelde dat het aanmaken van een e-mailaccount op naam van een andere persoon, met bedrieglijk opzet of met het oogmerk te schaden, manipulatie van computergegevens uitmaakt.[504] De rechtbank bevond U.T. bijgevolg schuldig aan de schending van de artikelen 193 en 210bis Sw..[505]

2.3 Vonnis van 29 augustus 2008 van de rechtbank van eerste aanleg te Dendermonde'

318. Een zaak die hierbij aansluit is de zaak van 29 augustus 2008, die voor de rechtbank van eerste aanleg te Dendermonde werd behandeld.[506] In casu had M.C., de beklaagde, de gegevens van het curriculum vitae van J.G. op Jobat, Stepstone en Eci gewijzigd, en bewuste taalfouten aangebracht. Verder wijzigde de beklaagde het paswoord van het slachtoffer zijn hotmailaccount. De beklaagde werd beschuldigd van inbreuken op de artikelen 210 bis§1 en 550bis §1 en §3 Sw.. Gezien de beklaagde, enerzijds, gegevens vervalst en, anderzijds, zich schuldig maakt aan externe hacking, werd de persoon in kwestie schuldig bevonden aan de tenlastelegging. Een opmerkelijk aspect van dit vonnis heeft betrekking op de bevoegdheidscriteria voor de correctionele rechtbanken, zoals voorzien in artikel 139 Sv..[507] In België wordt, wat betreft de bepaling van de plaats van het misdrijf, de ubiquiteitsleer toegepast. De ubiquiteitsleer wordt doorgaans echter op een zodanig soepele wijze geïnterpreteerd, waardoor deze meer weg heeft van de leer van de ondeelbaarheid . Op grond van deze leer wordt aangenomen dat de Belgische rechter kennis kan nemen van alle elementen van het misdrijf die een ondeelbaar geheel vormen met het misdrijf dat op Belgisch grondgebied werd gepleegd. De leer van de ondeelbaarheid mondt vervolgens vaak uit in de zgn. effectenleer.[508] In casu heeft de rechter moeten oordelen over al deze principes, en dit in een cyberspacecontext, wat allerminst evident is. De klacht werd neergelegd bij het parket van Dendermonde, waar het slachtoffer woonachtig was. Na onderzoek bleek dat de misdrijven

[504] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 563.
[505] Corr. Dendermonde 28 november 2005, *RABG* 2007, (427) 427.
[506] Rb. Dendermonde 29 augustus 2008, www.juridat.be, noot.
[507] Rb. Dendermonde 29 augustus 2008, www.juridat.be, noot.
[508] Rb. Dendermonde 29 augustus 2008, www.juridat.be, noot.

werden gepleegd op een computer die zich in Zaventem bevond, een gemeente die zich in het gerechtelijk arrondissement Brussel bevindt. Men kan zich in dit kader dan ook de vraag stellen in welke mate men feiten die worden gepleegd in Zaventem, kunnen vervolgd worden in Dendermonde. De rechter in kwestie heeft de territorialiteitsbeginselen in dit kader nauwgezet toegepast op een informaticacontext. Zo stelde de rechter dat het slachtoffer zijn laptop heeft aangezet in Dendermonde, waarna bleek dat zijn hotmailaccount gehacked was. De rechter oordeelde dat dit element een ondeelbaar geheel vormt met de handelingen die de verdachte heeft gesteld op zijn pc, in Zaventem. Op grond van deze redenering achtte de rechtbank zich territoriaal bevoegd.[509]

2.4 Vonnis van 14 november 2008 van de rechtbank van eerste aanleg te Dendermonde'

319. Een andere zaak is die van 14 november 2008 voor de rechtbank van eerste aanleg van Dendermonde.[510] Concreet ging het om een persoon die in zijn wagen op zijn laptop aan het surfen was. Een patrouille van de politie van Sint-Gillis-Waas heeft de persoon in kwestie daarover aangesproken, waarna bleek dat het surfen geschiedde op de draadloze verbinding 'lokaal internet, wifi 8'. De persoon in kwestie was m.a.w. aan het surfen op een onbeveiligd netwerk. De tenlastelegging in deze zaak betrof de inbreuk op artikel 550bis §1, eerste lid Sw., met name de ongeoorloofde toegang tot een informaticasysteem. In casu betreft het een externe hacking, de persoon in kwestie wetens en willens wist dat hij zich, zonder daartoe gerechtigd te zijn, toegang verschafte tot een informaticasysteem. Wat dit laatste betreft volgt de correctionele rechtbank hier de meerderheidsopvatting in de rechtspraak. Deze stelt namelijk dat de beklaagde strafbaar is, van zodra hij weten en willens in het informaticasysteem binnendringt.[511] Het is een vaak voorkomend misverstand, dat het gebruik maken van andermans draadloos netwerk zondermeer toegelaten is. Toch is dit niet zo onschuldig als het lijkt. Er wordt vaak vergeten welke gevolgen dit voor de houder van het onbeveiligd draadloos netwerk met zich kan meebrengen. Indien iemand bijvoorbeeld via zijn netwerk kinderpornografie download, zal bij een mogelijke IP-identificatie, de houder van het netwerk worden aangesproken. Dit terwijl deze laatste daar, in geen enkele opzicht, iets mee te maken heeft. De wet is in dit geval, naar mijn mening terecht, onverbiddelijk. De rechtbank oordeelde dan ook dat hij schuldig was aan de schending van dit artikel.

[509] Rb. Dendermonde 29 augustus 2008, www.juridat.be, noot.
[510] Rb. Dendermonde 14 november 2008, *Computerr.* 2009, (74) 74, noot L. DAUWE.
[511] Corr. Dendermonde 25 mei 2007, *TGR-TWVR* 2007, (351) 351.

2.5 Vonnis van 14 mei 2007 van de correctionele rechtbank te Dendermonde'

320. Dit vonnis had betrekking op een zaak waarbij de verdachten zich onder meer schuldig hadden gemaakt aan informaticabedrog.[512] Meer bepaald kopieerden zij bankkaarten door middel van technische middelen, waarna zij deze kaarten gebruikten om zich geld van anderen toe te eigenen. De verdachten in deze zaak gingen bijzonder geraffineerd te werk.[513] Ze plaatsten op de kaartlezers van de bankfilialen een toestel dat de magneetstrook van de bankkaart kopieerden.[514] Daarenboven bevestigden ze een minuscule camera bovenop de geldverdeler, waardoor ze de geheime code van de nietsvermoedende klanten konden zien. De beelden die de camera registreerde werden vervolgens draadloos doorgezonden naar een videorecorder. Met al deze gegevens in handen, haalden de verdachten meermaals geld van de rekening van de gedupeerden, telkens voor het maximaal beschikbare bedrag. Dat de verdachten bijzonder sluwe vossen waren, bleek uit het feit dat ze dit procedé tweemaal uitvoerden. Met name net voor, en net na middernacht. Op deze manier was het mogelijk om tweemaal het maximum bedrag van de rekening te halen, gezien dit op verschillende kalenderdagen gebeurde. De correctionele rechtbank heeft hen dan ook veroordeeld voor informaticabedrog, en eveneens voor hacking, en valsheid in informatica.[515] Voor de wetswijziging van 15 mei 2006 werd skimming enkel als informaticabedrog gecatalogeerd, indien de gegevens die men hierdoor had verkregen, hadden geleid tot een bedrieglijk vermogensvoordeel. De wet van 15 mei 2006 bracht hier verandering in. Vanaf er een bedoeling bestaat om een economisch voordeel te verwerven d.m.v. skimming, is dit strafbaar op grond van artikel 504quater Sw..[516]

2.6 Arrest van 10 september 2008 van het hof van beroep te Antwerpen

321. Dit arrest heeft, net als het vorige, betrekking op bankkaarten.[517] In deze zaak was er echter geen sprake van skimming. De verdachte in deze zaak had de bankkaart van het slachtoffer, buiten die zijn wil om, gebruikt om geld af te halen.[518] Het hof oordeelde dat dit een inbreuk is op artikel 504quater Sw..Het feit dat de bankkaart niet werd vervalst doet niet

[512] Corr. Dendermonde 14 mei 2007, *T. Strafr*. 2007, 403.
[513] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 564.
[514] Deze activiteit wordt 'skimming' genoemd.
[515] Corr. Dendermonde 14 mei 2007, *T. Strafr*. 2007, 403.
[516] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 564.
[517] Antwerpen 10 september 2008, *NC* 2009, 328.
[518] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 565.

ter zake, aldus het hof. Het gebruik maken van andermans bankkaart om zichzelf een onrechtmatig vermogensvoordeel te verschaffen, volstaat om zich schuldig te maken aan informaticabedrog.[519]

2.7 Vonnis van 8 januari 2008 van de correctionele rechtbank te Brussel

322. In dit vonnis betrof het een zaak van externe hacking. Meer bepaald had een werkgever zich toegang verschaft tot de privécomputer van één van zijn werknemers. De rechter oordeelde dat dit een inbreuk was op artikel 550bis Sw.[520] Het feit dat de werkgever dit deed, ongeacht zijn intentie, leidde tot deze tenlastelegging, des te meer omdat de toegang tot de privécomputer werd beschermd door een wachtwoord.[521]

2.8 Vonnis van 21 januari 2004 van de correctionele rechtbank te Hasselt

323. Waar het merendeel van de rechtspraak oordeelt dat een beklaagde zich schuldig maakt aan artikel 550bis Sw., van zodra hij wetens en willens een informaticasysteem binnendringt, wordt in dit arrest een afwijkende stelling geponeerd.[522] [523] De feiten zijn de volgende: de beklaagde was klant bij Bacob. Hij ontdekte echter dat hij het begunstigdenbestand van klanten van de Bacobbank, die eveneens internetbankierden, kon downloaden, waarna hij de rekeningnummers van begunstigden wijzigde. De beklaagde ging twee weken later naar zijn Bacobfiliaal, met de melding dat hun e-banking systeem verre van veilig was. De bediende van het plaatselijke filiaal wees hem erop dat hij dit kon melden bij 'Bacob Direct Net'. Een maand later had men bij Bacob begrepen hoe de vork aan de steel zat, en werd er klacht ingediend.[524] De correctionele rechtbank van Hasselt was, in deze zaak, de mening toegedaan dat het feit dat een informaticasysteem niet beveiligd is, met zich meebrengt dat de verdachte die het systeem binnendrong, geen kwaad opzet kan worden verweten. De gedachtengang is ietwat vreemd te noemen. Des te meer omdat de verdachte wel degelijk wist dat hij het netwerk binnendrong, net omdat dit onbeveiligd was. Hoe men dit gegeven dan ook heeft

[519] Antwerpen 10 september 2008, *NC* 2009, 328.
[520] Corr. Brussel 8 januari 2008, *JT* 2008, (337) 337, noot A. LEROY.
[521] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 565.
[522] Rb. Dendermonde 14 november 2008, *Computerr.* 2009, (74) 74, noot L. DAUWE.; Corr. Dendermonde 25 mei 2007, *TGR-TWVR* 2007, (351) 351.; Corr. Eupen 15 december 2003, *Computerr.* 2004, (129) 129, *RDTI* 2004, (61) 61, noot O. LEROUX.
[523] Corr. Hasselt 21 januari 2004, *Computerr.* 2004, 130, noot H. GRAUX.
[524] Corr. Hasselt 21 januari 2004, *Computerr.* 2004, 130, noot H. GRAUX.

kunnen kwalificeren als zijnde geen kwaad opzet, is mij een raadsel. De meerderheid van de rechtspraak volgt deze uitspraak dan ook niet.[525]

2.9 Vonnis van 10 januari 2008 van de correctionele rechtbank te Brussel

324. Deze zaak ging omtrent de hierna beschreven feiten. Tijdens een huiszoeking werden pc's in beslag genomen. De politiediensten wisten dat de verdachte gebruik maakte van hotmailaccounts, deze laatste wou deze wachtwoorden echter niet kenbaar maken.[526] Tijdens de huiszoeking was de politie echter gestoten op een document, waarop de wachtwoorden stonde vermeld. De verbalisanten gingen vervolgens over tot de exploitatie en doorzoeking van de hotmailaccounts.[527] De correctionele rechtbank heeft in dit kader een opmerkelijke beslissing genomen. Het stelde meer bepaald dat, indien er wordt gehandeld op grond van een geldig huiszoekingsbevel, in het raam waarvan het noodzakelijk is om de zoeking uit te breiden naar een informaticasysteem dat zich op een andere plaats bevindt, de onderzoekers daartoe kunnen overgaan zonder verdere formaliteiten, mits ze de voorwaarden beschreven in artikel 88ter §1 en §2 Sv. respecteren.[528] Vanuit de rechtsleer is er sterke kritiek gekomen op de uitspraak. De meerderheidsopvatting is immers de mening toegedaan dat de wetgever geen verlenging van de huiszoeking voor ogen had, maar wenste dat er een sui generis statuut werd verleend aan artikel 88ter Sv., waarbij vooraf een beslissing van de onderzoeksrechter is vereist. De beslissing die de correctionele rechtbank in dit kader nam, staat hier haaks tegenover.[529]

2.10 Arrest van 7 oktober 2003 van het hof van beroep te Antwerpen

325. De beklaagde in deze zaak had een website opgericht, illegalwebs.com. Via deze websites konden de gebruikers links bekomen, die verwezen naar pagina's met kinderporno als inhoud.[530] De beklaagde werd door de correctionele rechtbank van Hasselt veroordeeld voor het bezit en de verspreiding van kinderpornografie. De beklaagde tekende beroep aan

[525] Rb. Dendermonde 14 november 2008, *Computerr.* 2009, 74, noot L. DAUWE.; Corr. Dendermonde 25 mei 2007, *TGR-TWVR* 2007, 351.; Corr. Eupen 15 december 2003, *Computerr*. 2004, 129, *RDTI* 2004, 61, noot O. LEROUX.
[526] J. KEUSTERMANS en T. DE MAERE, "Tien jaar wet informaticacriminaliteit", *RW* 2010, (562) 568.
[527] Corr. Brussel 10 januari 2008, *T. Strafr*. 2008, 149.
[528] Corr. Brussel 10 januari 2008, *T. Strafr*. 2008, 149.
[529] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het einde van de tunnel", *T. Strafr*. 2008, 79-95.
[530] Antwerpen, 7 oktober 2003, *Computerr*. 2004, 85.

tegen dit vonnis bij het hof van beroep te Antwerpen, zonder succes.[531] In casu betreft het de bestraffing van een aanverwant misdrijf, met name de verspreiding van kinderpornografie in een informaticacontext.

2.11 Vonnis van 2 augustus 2009 van de correctionele rechtbank te Dendermonde'

326. Deze zaak was gericht tegen Yahoo! Inc., dat werd veroordeeld voor inbreuken op artikel 46bis Sv.. Meer bepaald had Yahoo! Inc. geweigerd bepaalde gegevens te verstrekken, in het kader van de medewerkingsverplichting.[532] Yahoo! Inc. tekende tegen dit vonnis beroep aan, en werd bij arrest van 30 juni 2010 door het hof van beroep te Gent vrijgesproken. Vervolgens werd er cassatieberoep ingesteld. Het Hof van Cassatie vernietigde het bestreden arrest van het hof van beroep te gent.[533]

3. CONCLUSIE

327. Als we de voorafgaande rechtspraak bekijken, kunnen we niet anders dan concluderen dat de wet inzake informaticacriminaliteit haar vruchten heeft afgeworpen.. De verschillende rechtbanken in ons land, op meerdere echelons, hebben succesvol gebruik weten te maken van de nieuwe strafbaarstellingen, die door de wet van 28 november 2000 werden ingevoerd. Waar de rechter zich, rond de eeuwwisseling, nog diende te behelpen met traditionele strafbaarstellingen, heeft hij nu een adequaat instrumentarium voorhanden.

Hoofdstuk 7: Conclusie

328. België gaf, wat de aanpak van cybercriminaliteit betreft, lange tijd blijk van een standvastige wil tot achterop hinken. De wet van 28 november 2000 inzake informaticacriminaliteit heeft daar op abrupte wijze verandering in gebracht. Waar België in de jaren '90 nog de slechte leerling van de klas was, hees het zich in 2000 naar een meer

[531] Antwerpen, 7 oktober 2003, *Computerr.* 2004, 85.
[532] Corr. Dendermonde 2 augustus 2009, www.juridat.be.
[533] Corr. Dendermonde 2 augustus 2009, www.juridat.be, gewijzigd door Gent 30 juni 2010, www.juridat.be, vernietigd door Cass. 18 januari 2011, www.juridat.be.

respectabelere positie. De wijzingen die de wet inzake informaticacriminaliteit invoerde, lijken succesvol te zijn. De wijzigingen op het vlak van het strafprocesrecht dienen positief benaderd te worden. De FCCU heeft met het databeslag, de netwerkzoeking, de medewerkingsverplichting e.d. adequate wapens voorhanden, in de strijd tegen cybercriminaliteit. Ook bij de parketten zien we een positieve evolutie. Er valt met name een stijgende tendens waar te nemen, voor wat betreft de instroom van informaticazaken. Uit de analyse van de rechtspraak blijkt dat ook de Belgische rechter zijn weg naar de nieuwe incriminaties heeft gevonden.

329. Toch is niet alles rozengeur en maneschijn. Wat het wetgevend kader betreft, is het wraakroepend dat er nog steeds geen uitvoeringsbesluit is tot stand gekomen omtrent de dataretentie. Een ander punt waar kritiek op zijn plaats is, betreft de situatie van de Computer Crime Units. Zowel de FCCU, als de RCCU's zijn hopeloos onderbemand, en hebben te weinig budget voorhanden. Ook het beperkte maatschappelijk bewustzijn omtrent cybercriminaliteit, is in dat opzicht schrijnend. Mijn interview met Luc Beirens had bij wijlen dan ook een scherpe ondertoon, wat niet hoeft te verbazen. Uit de voorbeelden die Luc Beirens mij aanreikte, bleek dat de activiteiten van de FCCU bij wijlen meer weg hebben van water naar de zee dragen, dan van mogelijkheden om effectief te kunnen optreden. De hoop tot verandering laaide dan ook op, toen België begin van dit jaar collectief van zijn stoel viel door de historie omtrent het Tor-netwerk. Politici sprongen op de barricades, de FCCU zou meer mensen en middelen krijgen om dit soort van feiten aan te pakken. Na verloop van tijd ging de storm echter liggen, waarna het Tor-netwerk uit de media verdween. Hand in hand met de media-aandacht, verdwenen tevens de goede voornemens en krachtige uitspraken van de politici. De zo verhoopte verandering, kwam er niet. Deze gang van zaken hoeft niet te verbazen, het maakt immers deel uit van het politieke spel. Niettemin dient er gehoopt te worden op fundamentele veranderingen, anders dreigen de frustraties onder de FCCU mensen af te glijden naar een gevoel van gelatenheid.

DEEL VI: De Nederlandse aanpak inzake cybercriminaliteit

Hoofdstuk 1: Inleiding

330. In dit deel zal de Nederlandse aanpak aangaande cybercriminaliteit besproken worden. Net als bij de bespreking van de Belgische situatie, zal ook hier achtereenvolgend de relevante wetgeving, de opsporing en de vervolging, alsmede de straftoemeting besproken worden. De uiteenzetting in dit deel zal zich beperken tot de belangrijkste aspecten van de Nederlandse aanpak.

Hoofdstuk 2: Het wettelijk kader

1. MATERIEEL STRAFRECHT

331. Waar België in de jaren '90 lange tijd blijk gaf van een standvastige wil tot achterop hinken, was Nederland op dat punt al bezig met wetgevende initiatieven. In Nederland werd immers al zeer vroeg onderkend dat het Nederlandse Wetboek van Strafrecht niet voldeed om op te treden tegen cybercriminaliteit.[534] Op 13 november 1985 werd de Commissie Computercriminaliteit opgericht. Deze commissie werd ook wel de 'Commissie Francken' genoemd, naar haar voorzitter.[535] Na het voorbereidend werk van de Commissie Computercriminaliteit, waarvan in 1987 het rapport verscheen, zag de wet computercriminaliteit (I) in 1993 het levenslicht.[536] Deze wet vulde het Wetboek van Strafrecht aan met een aantal nieuwe delicten, en het Wetboek van Strafvordering met een aantal nieuwe bevoegdheden voor de opsporingsdiensten. Het valt op dat deze evolutie vergelijkbaar is met diegene die België heeft doorgemaakt, zij het een kleine tien jaar vroeger.

332. De computervredebreuk, het verspreiden van virussen, het beschadigen van gegevens, het onbevoegd aftappen van gegevensverkeer en het vervalsen van betaalkaarten, waren de nieuwe incriminaties die de wet van 1993 invoerde. Wat het strafprocesrecht betreft kwamen er nieuwigheden, zoals het aftappen van elke vorm van gegevensverkeer, het bevel tot

[534] H.W.K. KASPERSEN, *Schriftelijke leergang Nieuwe Telecomwet*, Hilversum, Broadcast Press, 2004, http://pubs.cli.vu/pub168.php.
[535] P. KLEVE, R.V. DE MULDER en C. VAN NOORTWIJK, "ICT Criminaliteit", in E.R. MULLER, J.P. VAN DER LEUN, L.M. MOERINGS en P.J.V. VAN CALSTER, *Criminaliteit: criminaliteit en criminaliteitsbestrijding in Nederland*, Alphen aan den Rijn, Kluwer, 2010, (259) 270.
[536] Wet 24 december 1992, *Stb.* 1993, 33.

uitlevering van gegevens, het bevel tot toegangsverschaffing tot computers en de netwerkzoeking. [537] Waar H.W.K. Kaspersen in 1993 nog hoopvol stelde: *"De wet computercriminaliteit is er, nu de boeven nog"*, bleek enkele jaren later dat er een aanpassing vereist was. [538] Nog geen 6 jaar later waren de boeven van Kaspersen er in grote getalen en gebruikten ze steeds nieuwere vormen van cybercriminaliteit.[539] Op 8 juli 1999 werd daarom een nieuw wetsvoorstel bij de Tweede Kamer ingediend, genaamd Computercriminaliteit II.[540] Het wetsvoorstel omvat een aantal aanvullingen, reparaties en verbeteringen van de materiële strafbepalingen. Gezien in datzelfde tijdsbestek het Cybercrime-Verdrag van de Raad van Europa tot stand kwam, werd de behandeling van het wetsvoorstel uitgesteld tot 2004. Het Cybercrime-Verdrag is mede geïmplementeerd in de Wet Computercriminaliteit II.[541]

333. De concrete strafbaarstellingen zijn in grote lijnen dezelfde als in België. Net zoals in de relevante Belgische regelgeving, maakt de Nederlandse wetgever een opsplitsing in vier categorieën:[542]

- binnendringen in een geautomatiseerd werk;
- stoornis in de gang of werking van een geautomatiseerd werk;
- onbruikbaar maken, veranderen of aantasten van gegevens;
- afluisteren.

334. Bovenstaande gedragingen zijn te catalogeren onder de noemer 'cybercriminaliteit in de enge zin'. Naast deze kernbepalingen, heeft de Nederlandse wetgever ook cybercriminaliteit in de ruime zin willen aanpakken. Deze misdrijven, zoals bijvoorbeeld valsheid in geschrifte of fraude, zijn vervat in de traditionele artikelen gericht op deze feiten. In de respectievelijke artikelen wordt vermeld dat de feiten ook strafbaar zijn indien zij worden gepleegd langs geautomatiseerde weg.

[537] H.W.K. KASPERSEN, "De wet computercriminaliteit is er- nu de boeven nog", *Computerr.* 1993, (134) 137.
[538] H.W.K. KASPERSEN, "De wet computercriminaliteit is er- nu de boeven nog", *Computerr.* 1993, (134) 137.
[539] C.P.M. CLEIREN en J.F. NIJBOER, *Strafrecht: tekst en commentaar*, Deventer, Kluwer, 2008, 1409.
[540] B.J. KOOPS en M.H.M. SCHELLEKENS, "Computercriminaliteit II: de boeven zijn er – nu de wet weer", *Nederlands Juristenblad* 1999, (1764) 1764. (1764- 1772)
[541] Wet 1 juni 2006 inzake computercriminaliteit II, *Stb.* 2006.
[542] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 12.

1.1 Binnendringen in een geautomatiseerd werk

335. Artikel 138ab van het Wetboek van Strafrecht stelt het binnendringen in een geautomatiseerd werk strafbaar. Met dit artikel heeft de Nederlandse wetgever elke vorm van opzettelijk en wederrechtelijk binnendringen strafbaar gesteld, ook in het geval waarbij er geen beveiliging wordt doorbroken.[543] Dit laatste element is toegevoegd door de wet Computercriminaliteit II, dat de omschrijving van computervredebreuk daarmee streng verscherpte. Artikel 138ab valt uiteen in drie punten. Vooreerst wordt er, in het eerste lid, het binnendringen in een geautomatiseerd werk op een algemene wijze omschreven. Dit wordt gestraft met een gevangenisstraf van ten hoogste één jaar, of een geldboete van categorie vier, wat neerkomt op 19.000 euro. Het tweede lid omschrijft het geval waarin er wordt binnengedrongen in een geautomatiseerd werk, waarna er vervolgens gegevens worden gekopieerd. Dit wordt bestraft met een gevangenisstraf van maximaal vier jaar, of een geldboete van 19.000 euro. Het derde lid omschrijft tenslotte het binnendringen in een geautomatiseerd werk, via een openbaar telecommunicatienetwerk, om het vervolgens verder te hacken. De straffen die hieraan worden gekoppeld zijn dezelfde, als die voorzien voor het tweede lid. Het feit dat lid twee en drie zwaarder wordt bestraft, ligt aan het feit dat dit verzwarende omstandigheden uitmaken.[544]

1.2 Stoornis in de gang of werking van een geautomatiseerd werk

336. Het belemmeren van de toegang tot, of het gebruik van een geautomatiseerd werk door het aanbieden of toezenden van gegevens is strafbaar gesteld in artikel 138b van het Wetboek van Strafrecht. Artikel 138b bepaalt twee criteria voor strafbaarstelling. Enerzijds, de toegang tot of het gebruik van een geautomatiseerd werk opzettelijk en wederrechtelijk belemmeren. Anderzijds, dit laten geschieden door middel van het aanbieden of toezenden van gegevens.[545] Deze bepaling is vooral gericht tegen virussen, Trojaanse paarden en (D)DoS-aanvallen.[546] Aan deze feiten wordt een gevangenisstraf gekoppeld van maximaal één jaar, of een

[543] P. KLEVE, R.V. DE MULDER en C. VAN NOORTWIJK, "ICT Criminaliteit", in E.R. MULLER, J.P. VAN DER LEUN, L.M. MOERINGS en P.J.V. VAN CALSTER, *Criminaliteit: criminaliteit en criminaliteitsbestrijding in Nederland*, Alphen aan den Rijn, Kluwer, 2010, (259) 270.
[544] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 12.
[545] P. KLEVE, R.V. DE MULDER en C. VAN NOORTWIJK, "ICT Criminaliteit", in E.R. MULLER, J.P. VAN DER LEUN, L.M. MOERINGS en P.J.V. VAN CALSTER, *Criminaliteit: criminaliteit en criminaliteitsbestrijding in Nederland*, Alphen aan den Rijn, Kluwer, 2010, (259) 270.
[546] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 12.

geldboete van maximaal 19.000 euro. Het verstoren van de werking van een geautomatiseerd werk is eveneens strafbaar gesteld in de artikelen 161sexies en 161septies van het Wetboek van Strafrecht. De wetgever maakt een onderscheid naargelang de situatie waarin iemand een werk opzettelijk vernielt, beschreven in artikel 161sexies, en de situatie waarin de dader nalatig is, zoals beschreven in artikel 161septies. De strafmaat in deze artikelen varieert naargelang de gevolgen die de inbreuk met zich meebrengt. Afhankelijk van de gevolgen, kan de strafmaat variëren van een gevangenisstraf van ten hoogste één jaar tot vijftien jaar, of een geldboete van 19.000 euro tot 76.000 euro.[547]

1.3 Onbruikbaar maken, veranderen of aantasten van gegevens

337. Het onbruikbaar maken, veranderen of anderszins aantasten van gegevens heeft de Nederlandse wetgever strafbaar gesteld in de artikelen 350a en 350b van het Wetboek van Strafrecht. Ook hier maakt de wetgever een onderscheid tussen de situatie waarin dit opzettelijk gebeurt, en de situatie waarin dit niet opzettelijk gebeurt, maar waarin er wel sprake is van schuld.[548] De twee voorgaande artikelen stellen twee soorten gedragingen strafbaar. Enerzijds, het aantasten van gegevens en, anderzijds, het ter beschikking stellen van en verspreiden van gegevens die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd netwerk, zoals virussen, wormen en andere malware.[549] Indien er sprake is van opzet, riskeert de dader een gevangenisstraf van maximum twee jaar, of een geldboete van 19.000 euro. De gevangenisstraf kan worden verhoogd tot vier jaar, indien er een openbaar telecommunicatienetwerk wordt gebruikt, en de gegevens ernstig worden beschadigd.[550] Het verspreiden van malware wordt bestraft met een gevangenisstraf van ten hoogste vier jaar, of een geldboete van 76.000 euro. Indien er geen sprake is van opzet, maar wel van schuld, liggen de straffen aanzienlijk lager. De gevangenisstraffen in dit kader zijn beperkt tot maximum één maand, de geldboetes tot 3.800 euro.[551]

[547] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 12.
[548] P. KLEVE, R.V. DE MULDER en C. VAN NOORTWIJK, "ICT Criminaliteit", in E.R. MULLER, J.P. VAN DER LEUN, L.M. MOERINGS en P.J.V. VAN CALSTER, *Criminaliteit: criminaliteit en criminaliteitsbestrijding in Nederland*, Alphen aan den Rijn, Kluwer, 2010, (259) 270.
[549] H. FRANKEN en H.W.K. KASPERSEN, "Strafrecht en opsporing in computernetwerken", in H. FRANKEN, H.W.K. KASPERSEN en A.H. DE WILD, *Recht en computer*, Deventer, Kluwer, 2004, (385) 400.
[550] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 25.
[551] P. KLEVE, R.V. DE MULDER en C. VAN NOORTWIJK, "ICT Criminaliteit", in E.R. MULLER, J.P. VAN DER LEUN, L.M. MOERINGS en P.J.V. VAN CALSTER, *Criminaliteit: criminaliteit en criminaliteitsbestrijding in Nederland*, Alphen aan den Rijn, Kluwer, 2010, (259) 270.

1.4 Afluisteren

338. Het aftappen en opnemen van gegevens in relatie tot een geautomatiseerd netwerk is strafbaar gesteld in de artikelen 139c, 139d, en 139e van het Wetboek van Strafrecht. Het aftappen en opnemen van gegevens, zoals bepaald in artikel 139c, is strafbaar gesteld met een gevangenisstraf van maximum één jaar, of een geldboete van 19.000 euro.[552] Het plaatsen van opname-, aftap-, of afluisterapparatuur, zoals voorzien in artikel 139d, is strafbaar gesteld met een gevangenisstraf van ten hoogste vier jaar, of een geldboete van 19.000 euro. Het voorhanden hebben en gebruiken van gegevens die door onrechtmatig afluisteren, aftappen of opnemen zijn vergaard, wordt, zoals voorzien in artikel 139e, bestraft met een gevangenisstraf van maximum zes maanden, of een geldboete van 19.000 euro. In dit kader heeft de Nederlandse wetgever eveneens bepalingen ingevoerd omtrent de schending van de geheimhouding. Dit zowel wat betreft gegevens verkregen uit een misdrijf, als uit een arbeidsovereenkomst. Deze bepalingen zijn vervat in artikel 273 van het Wetboek van Strafrecht, en worden bestraft met een gevangenisstraf van maximum zes maanden, of een geldboete van 19.000 euro.[553]

2. STRAFPROCESRECHT

339. Naast de wijzigingen die het Wetboek van Strafrecht heeft ondergaan, naar aanleiding van de wet Computercriminaliteit I en II, is ook het Wetboek van Strafvordering aangepakt. Het Wetboek van Strafvordering laat de rechter-commissaris, officier van justitie, hulpofficier van justitie en opsporingsambtenaar het doorzoeken van plaatsen toe om gegevens vast te leggen die op een gegevensdrager zijn opgeslagen, zoals bepaald in artikel 125i.[554] Artikel 125j, lid 1 stelt dat het doorzoeken van een geautomatiseerd werk dat met een netwerk verbonden is, eveneens op afstand mag plaatsvinden, als dit redelijkerwijs nodig is om de waarheid aan de dag te brengen.[555] Verder stelt artikel 125j, lid 2 dat het onderzoek zich moet beperken tot geautomatiseerde werken waar de normale gebruikers van de doorzochte computer rechtmatig toegang toe hebben, vanaf de plaats waar de doorzoeking plaatsvindt.

[552] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 26.
[553] P. KLEVE, R.V. DE MULDER en C. VAN NOORTWIJK, "ICT Criminaliteit", in E.R. MULLER, J.P. VAN DER LEUN, L.M. MOERINGS en P.J.V. VAN CALSTER, *Criminaliteit: criminaliteit en criminaliteitsbestrijding in Nederland*, Alphen aan den Rijn, Kluwer, 2010, (259) 273.
[554] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 13.
[555] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 8.

340. Artikel 125k stelt dan weer dat een persoon, maar niet de verdachte, die kennis draagt van de wijze van beveiliging van een geautomatiseerd werk of gegevens, het bevel kan krijgen toegang te verschaffen tot de geautomatiseerde werken of gegevens. In het kader van een onderzoek kan het ook nodig zijn om computergegevens of gegevensdragers veilig te stellen voor verder onderzoek, of als bewijs. Dit wordt geregeld in artikel 94 van het Wetboek van Strafvordering.[556] Daarnaast kan de politie ook bevelen dat de eigenaar de harde schijf van een computer afstaat. Ook kunnen de opsporingsdiensten een service provider verplichten het dataverkeer van een verdachte op te nemen. Belangrijk is dat ook bij de normale doorzoekingbevoegdheden computers kunnen worden onderzocht en gegevens kunnen worden gekopieerd, zoals is vastgelegd in de Wet computercriminaliteit van 1993. Verder zijn de meeste opsporingsbevoegdheden van toepassing, door de vermelding van bijna alle delicten in het Wetboek van Strafvordering. [557]

3. CONCLUSIE

341. Als we naar de hierboven beschreven bepalingen kijken, kunnen we niet anders dan vaststellen dat deze in grote lijnen overeenkomen met de bepalingen uit het Belgische Strafwetboek. Dit is echter niet onlogisch. Het Cybercrime-Verdrag is door beide landen opgenomen in de nationale wetgeving, waardoor de bepalingen enigszins gestroomlijnd zijn. We zien dit trouwens niet alleen in Nederland. De meeste Europese landen geven dezelfde invulling aan de verschillende inbreuken. Wat wel verschilt, is dat de maximumstraffen die in Nederland voor dergelijke feiten worden opgelegd, relatief hoger liggen dan in België. Eind juli 2010 publiceerde het ministerie van Justitie een wetsontwerp omtrent de versterking van de bestrijding van computercriminaliteit. Het lijkt er dus sterk op dat Nederland in de nabije toekomst het ontstaan van een nieuwe wet Computercriminaliteit III zal mogen aanschouwen.[558]

[556] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 89.
[557] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 13.
[558] B.J. KOOPS, "Tijd voor Computercriminaliteit III", *Nederlands Juristenblad* 2010, (2461) 2466.

Hoofdstuk 3: De opsporing en vervolging van cybercriminaliteit in Nederland

1. DE GEÏNTEGREERDE SAMENWERKING

342. Cybercriminaliteit is al vele jaren een beleidsprioriteit in Nederland. In 2008 werd er, onder de vleugels van het Openbaar Ministerie, een intensiveringsprogramma 'Cybercrime' op poten gezet.[559] In dit programma werden miljoenen euro's gepompt. Het doel van het Openbaar Ministerie bestond er in de capaciteit en kennis te vergroten, om computercriminaliteit aan te pakken.[560] Er werden cybercrime-officieren en -secretarissen, beleidsmedewerkers en criminologen met een cybercrime-taak aangesteld.[561] Elk regioparket kreeg zijn cybercrime-officier, en er werd eveneens werk gemaakt van innovatie en opleiding.[562] Naast dit staaltje van proactief beleid, zijn er eveneens investeringen gebeurd op het punt van het Landelijk Parket, waar een kennis- en expertisecentrum voor cybercrime is opgericht.[563] Procureur-generaal Hans Moraal verdedigt de keuze voor deze investeringen. Laatstgenoemde stelde immers vast dat de doorsnee rechercheur aan 'koudwatervrees' leidt, als het op cybercriminaliteit aankomt. De situatie wordt echter onhoudbaar wanneer zij bij elke concrete zaak dienen te gaan aankloppen bij de specialisten ter zake, zoals het Team High Tech Crime van het Korps Landelijke Politiediensten, of het Nederlands Forensisch Instituut. Hans Moraal is de mening toegedaan dat deze twee instanties nooit meer dan het topje van de ijsberg voor hun rekening kunnen nemen. Waar het Team High Tech Crime zich bezighoudt met de opsporing van zware georganiseerde criminaliteit, dienen ook minder zware vormen van cybercriminaliteit aangepakt te worden. Dit vereist een breed gespreide deskundigheid. Daarom heeft men in Nederland geopteerd om alle medewerkers ICT-kennis bij te brengen. Het Openbaar Ministerie, het Landelijk Parket, Hoffmann bedrijfsrecherche, Digital Intelligence en IT beveiligingsbedrijf FOX IT hebben een SSR-leergang ontwikkeld, die onlangs is begonnen, met onderwerpen als ICT als doelwit, aanpak van botnets, internetgerelateerde fraude en kinderporno.[564] Binnen het intensiveringsprogramma hebben tevens drie proeftuinen gedraaid. Proeftuin 'Zambezi' had betrekking op het thema

[559] P. VERMAAS, "High Tech Crime", *Openbaar Ministerie: Opportuun* 2008, (20) 20.
[560] A. BRUINS, "Law and order in cyberspace", *Mr. Magazine* 2010, (28) 29.
[561] Openbaar Ministerie, "Intensief samenwerken tegen de ondermijnende en georganiseerde criminaliteit: aanpak cybercrime", *Twee weten meer dan één* 2012, (12) 13.
[562] A. BRUINS, "Law and order in cyberspace", *Mr. Magazine* 2010, (28) 28.
[563] A. BRUINS, "Law and order in cyberspace", *Mr. Magazine* 2010, (28) 29.
[564] A. BRUINS, "Law and order in cyberspace", *Mr. Magazine* 2010, (28) 29.

kinderporno, proeftuin 'Landelijk Meldpunt Internetgeralteerde Fraude' op het thema van fraude op het internet, en proeftuin 'Taurus' op het gebied van high-tech crime.[565] Dergelijke proeftuinen zijn leeromgevingen waarin het Openbaar Ministerie en de politie samenwerken. Het gaat in de proeftuinen niet alleen om het opsporen van criminelen, maar om innovatieve opsporingsmethoden met andere partners als het bestuur en internetproviders.[566]

2. DE OPSPORINGSINSTANTIES

2.1 Korps Landelijke Politiediensten

343. Het KPLD voert politietaken uit die een specialistisch karakter hebben of een bijzondere organisatie vergen. Ook taken die de grenzen van de politieregio's overschrijden en een nationaal of internationaal karakter hebben vallen onder hun bevoegdheidssfeer. Het KPLD richt zich op zware georganiseerde criminaliteit en terrorisme. Het heeft een landelijk Meldpunt Cybercrime, waar burger melding kunnen maken van computercriminaliteit.[567]

2.2 Nationaal Team High Tech Crime

344. Het Nationaal Team High Tech Crime is een onderdeel van de Dienst Nationale Recherche. Deze dienst ressorteert binnen de hierboven besproken KPLD. Het Nationaal Team High Tech Crime is een gespecialiseerd team van digitaal rechercheurs, dat vooral vormen van cybercriminaliteit onderzoekt waarbij zware en georganiseerde misdaad een rol speelt.[568] Ook vormen van cybercriminaliteit die een, al dan niet potentieel, gevaar inhouden voor de nationale veiligheid of de vitale belangen, vallen binnen hun werkingssfeer. Het team is daarenboven, internationaal gezien, het eerste aanspreekpunt voor buitenlandse opsporingsdiensten.[569] Het dient beschouwd te worden als de Nederlandse variant van de Federal Computer Crime Unit. Eind 2011 waren er dertig operationele rechercheurs aan het werk bij het Nationaal Team High Tech Crime. In januari 2012 werd echter aangekondigd dat

[565] Openbaar Ministerie, "Intensief samenwerken tegen de ondermijnende en georganiseerde criminaliteit: aanpak cybercrime", *Twee weten meer dan één* 2012, (12) 14.
[566] Openbaar Ministerie, "Intensief samenwerken tegen de ondermijnende en georganiseerde criminaliteit: aanpak cybercrime", *Twee weten meer dan één* 2012, (12) 14.
[567] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 123.
[568] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 125.
[569] M. SCHUIJERS en R. JONGMAN, "Speciale uitgave Team High Tech Crime/ Team Bestrijding Kinderporno en Kindersekstoerisme", *KPLD Magazine* 2012, (1) 7.

de KLPD een wervingsactie had gestart voor dertig nieuwe digitaal rechercheurs. Het personeelsbestand zou met andere woorden worden verdubbeld. Op deze manier wil het team de aanpak van cybercriminaliteit op een grotere schaal aanpakken. Het doel is om in 2015 twintig grote internationale zaken te kunnen behandelen. Het doel voor 2012 werd gesteld op tien zaken.[570]

2.3 Team Bestrijding Kinderporno en Kindersekstoerisme

345. Het Team Bestrijding Kinderporno en Kindersekstoerisme maakt eveneens deel uit van de Dienst Nationale Recherche. Het landelijke team houdt zich bezig met complexe opsporingsdossiers met een internationaal karakter. Bovendien komt alle informatie uit binnen- en buitenland hier samen, wat dit team het kenniscentrum bij uitstek maakt voor wat betreft kinderpornografie en kindersekstoerisme.[571] In januari 2012 werd, net als bij het Nationaal Team High Tech Crime, een aanzienlijke personeelsuitbreiding aangekondigd, van elf naar veertig.[572]

3. DE VERVOLGING

346. Het Openbaar Ministerie is verantwoordelijk voor de vervolging van cybcercriminaliteit. Waar de Belgische parketten bij de rechtbanken van eerste aanleg statistische gegevens bijhouden omtrent informaticacriminaliteit, gebeurt dit in Nederland niet. Er zijn statistieken te vinden, maar deze maken geen onderscheid tussen de feiten die al dan niet in een informaticacontext zijn gepleegd.

[570] O. VAN MILTENBURG, "KLPD gaat aantal digitale rechercheurs verdubbelen", *Volkskrant* 3 januari 2012, www.volkskrant.nl.
[571] M. SCHUIJERS en R. JONGMAN, "Speciale uitgave Team High Tech Crime/ Team Bestrijding Kinderporno en Kindersekstoerisme", *KPLD Magazine* 2012, (1) 10.
[572] O. VAN MILTENBURG, "KLPD gaat aantal digitale rechercheurs verdubbelen", *Volkskrant* 3 januari 2012, www.volkskrant.nl.

4. ANDERE INSTELLINGEN

4.1 Govcert.nl

347. Govcert.nl was tot 2012 het Computer Emergency Response Team van de Nederlandse overheid. Het platform zorgde voor ondersteuning van overheidsinstanties in het voorkomen en afhandelen van ICT-gerelateerde veiligheidsincidenten, en dit vierentwintig uur per dag, zeven dagen op zeven. Vanaf 1 januari 2012 is Govcert.nl geïntegreerd in het Nationaal Cyber Security Centrum van Nederland, dat hierna zal besproken worden. Wat betreft de internationale samenwerking, zal Govcert.nl zijn activiteiten verderzetten onder de naam NCSC-NL.[573]

4.2 Nationaal Cyber Security Centrum

348. Het Nationaal Cyber Security Centrum, of NCSC, is een gloednieuw platform, dat begin dit jaar werd opgericht. Het doel van het NCSC bestaat erin de weerbaarheid van de Nederlandse samenleving in een informatica-context te vergroten. Ze beogen dit door middel van samenwerking met de bedrijven, de overheid en de wetenschap. Het NCSC ondersteunt daarenboven de overheid, en organisaties met een vitale functie in de samenleving, door het verstrekken van advies en expertise in het geval van nakende dreigingen. Daarnaast speelt preventie en bewustwording ook een grote rol, waarbij het NCSC de bevolking, de overheid en het bedrijfsleven voorziet van informatie en advies. Het NCSC is daarenboven het centrale meld- en informatiepunt voor ICT-dreigingen en –veiligheidsincidenten.[574]

5. DE AANPAK VAN BREDOLAB: EEN SUCCESVERHAAL

349. Dat de aanpak van de Nederlanders ten aanzien van cybercriminaliteit werkt, werd in oktober 2010 duidelijk. Het botnet Bredolab werd opgerold door een samenwerkingsverbond van het Team High Tech Crime, Govcert.nl, Leaseweb, het NFI en Fox-IT. De manier waarop dit geschiedde was op z'n minst opmerkelijk te noemen. De verdachten maakten gebruik van een kleine honderdvijftig servers, waardoor ze sinds juli 2009 ten minste dertig miljoen

[573] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 123.
[574] Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 124.

computerinfecties veroorzaakten. Om het botnet neer te halen, maakte de KPLD gebruik van het botnet zelf, door eigen software op het botnet te installeren, waardoor er naar alle geïnfecteerde computers een melding werd gestuurd dat deze besmet waren. Op deze manier kon de KPLD het netwerk de das omdoen, en het brein achter het Bredolab, een Armeen, opsporen en in de boeien slaan. De manier waarop de KPLD dit bewerkstelligde, ging niet onopgemerkt voorbij.[575] Zo werd er beweerd dat de politie de wet zou overtreden hebben, door op het botnet in te breken. Het Openbaar Ministerie ontkrachtte deze kritiek echter, door te stellen dat dit niet strafbaar is, gezien de politie op deze wijze de schade wou beperken. Het Openbaar Ministerie catalogeerde de actie van de KPLD, met enig gevoel voor humor, als een legitieme digitale zaakwaarneming. Ongeacht de controverse die deze actie met zich meebracht, kan niet anders dan besloten worden dat dit een hele succesvolle operatie was, en tevens een opsteker voor de KPLD.[576]

Hoofdstuk 4: De straftoemeting door de rechter

1. BESPREKING VAN DE RELEVANTE RECHTSPRAAK

1.1 Arrest van 21 november 2006 van het Gerechtshof te Arnhem

350. In deze zaak had de verdachte zijn ex-vriendin gedurende zeven maanden belaagd. Tevens maakte hij enkele e-mailaccounts aan, waarmee hij lasterlijke berichten verstuurde in haar naam. De verdachte ging echter nog verder door allerhande advertenties op seks- en SMwebsites te plaatsen. De verdachte werd veroordeeld voor hacking, op grond van artikel 138ab van het Wetboek van Strafrecht. Het hof veroordeelde de man in kwestie tot een gevangenisstraf van vijf maanden, en de betaling van een geldboete van 2.500 euro.[577]

[575] M. HIJINK, "De politie mag een beetje terughacken", *NRC Handelsblad* 29 oktober 2010, www.nrc.nl.
[576] M. SCHUIJERS en R. JONGMAN, "Speciale uitgave Team High Tech Crime/ Team Bestrijding Kinderporno en Kindersekstoerisme", *KPLD Magazine* 2012, (1) 8.
[577] Arnhem 21 november 2006, www.rechtspraak.nl.

1.2 Vonnis van 8 december 2010 van de rechtbank van eerste aanleg te Utrecht

351. De verdachte in deze zaak had in 2009 OV-chipkaarten, die recht geven op een treinrit, gehacked en vervalst. Daarenboven had de verdachte zich schuldig gemaakt aan computervredebreuk. De rechtbank oordeelde dat de verdachte bewust dergelijke feiten had begaan. De verdachte stelde echter dat hij hiermee de tekortkomingen van de OV-chipkaarten wilde aantonen. De rechtbank hechtte hier geen belang aan. De verdachte werd dan ook op grond van artikel 138ab van het Wetboek van Strafrecht veroordeeld tot een gevangenisstraf van één maand voorwaardelijk.[578]

1.3 Arrest van 23 maart 2012 van het Gerechtshof te 's-Gravenhage

352. In deze zaak hadden de verdachten zich schuldig gemaakt aan het maken en verspreiden van een computervirus en een Trojaans paard. Het doel hiervan was wachtwoorden op te vangen en door te zenden naar de verdachten. Het hof was van oordeel dat de verdachten hiervoor hun kennis van informatie-technologie had misbruikt, en veroordeelde hen, op grond van artikel 138b van het Wetboek van Strafrecht, tot een gevangenisstraf van zevenhonderddertig dagen.[579]

2. CONCLUSIE

353. Net zoals dat voor België het geval was, lijken de Nederlandse rechters op een correcte manier toepassing te maken van de verschillende incriminaties. Zaken omtrent cybercriminaliteit komen vlot voor de rechtbanken, en worden adequaat afgehandeld. Op zich is dit ook niet meer dan normaal. Nederland kent immers al sinds 1993 bepalingen omtrent het strafbaar stellen van cybercriminaliteit, waardoor de rechters de tijd hebben gekregen om zich in te werken, alvorens de cybercriminelen in grote getalen hun intrede deden.

[578] Rb. Utrecht 8 december 2010, www.rechtspraak.nl.
[579] 's-Gravenhage 23 maart 2012, www.rechtspraak.nl.

Hoofdstuk 5: Conclusie

354. Wat de bepalingen van het materiële strafrecht en het strafprocesrecht betreft, kunnen we grote gelijkenissen waarnemen tussen de Belgische en de Nederlandse regelgeving. Het Cybercrime-Verdrag heeft hierin een grote rol gespeeld. Op het vlak van de opsporing van cybercriminaliteit zijn er daarentegen wel aanzienlijke verschillen tussen beide landen. Het mag gezegd worden dat Nederland, wat de opsporing van cybercriminaliteit betreft, een voortrekkersrol vervult. Nederland heeft van cybercriminaliteit een prioriteit gemaakt, en dat vertaalt zich op verschillende manieren. Binnen de Dienst Nationale Recherche van de KPLD, werden, met het Team High Tech Crime en het Team Bestrijding Kinderporno en Kindersekstoerisme, twee gespecialiseerde eenheden opgericht. De personeelsbezetting binnen deze twee teams is begin 2012 aanzienlijk uitgebreid. Het Nationaal Team High Tech Crime heeft nu zestig operationele rechercheurs, het Team Bestrijding Kinderporno en Kindersekstoerisme veertig. De FCCU dient het daarentegen te stellen met 25 operationele personeelsleden. Ook wat scholing en vorming betreft, staat Nederland vele malen verder dan België. Nederland heeft goed begrepen dat de politie op elk echelon over ICT-know-how dient te beschikken, en organiseert in dat kader dan ook een SSR-leergang, georganiseerd in samenwerking met privé-bedrijven, voor alle politiemensen. In België gebeurt deze scholing volledig intern, en minder doorgedreven dan in Nederland. Daarnaast wordt er in Nederland geïnvesteerd in een brede omkadering en ondersteuning, zoals blijkt uit de oprichting van het Nationaal Cyber Security Centrum. Daarnaast heeft Nederland ook een team voor digitale expertise, binnen het forensisch laboratorium. Dit alles draagt er toe bij dat we alleen maar kunnen concluderen dat Nederland, wat de opsporing van cybercriminaliteit betreft, op een veel hoger niveau speelt dan België. Wat de vervolging betreft, gaat de vergelijking tussen beide landen beter op. Zowel de Nederlandse als de Belgische rechters maken adequaat en succesvol gebruik van de strafbaarstellingen die ze voorhanden hebben.

DEEL VII: De aanpak van de Verenigde Staten inzake cybercriminaliteit

Hoofdstuk 1: Inleiding

355. In dit deel zal op summiere wijze worden nagegaan op welke wijze de Verenigde Staten cybercriminaliteit een halt proberen toe te roepen. Gelijklopend met de bespreking van de Belgische en de Nederlandse context, zal ook hier de relevante wetgeving, evenals de opsporing, de vervolging en de straftoemeting besproken worden. In dit deel zal een beeld geschetst worden van de situatie op het federale niveau.

Hoofdstuk 2: Het wettelijk kader

1. MATERIEELRECHTELIJKE BEPALINGEN

1.1 The Computer Fraud and Abuse Act

356. Gezien de Verenigde Staten een 'common law' rechtstraditie kent, heeft de wetgeving een ander vorm dan deze die we in België en Nederland kennen. Wat het materiële strafrecht betreft, werd in de VS de basis gelegd in het jaar 1986, met de 'Computer Fraud and Abuse Act', welke werd opgenomen in artikel 18 US Code s.1030.[580] Deze Act werd initieel in 1984 aangenomen als de 'Counterfeit Access Device and Computer Fraud and Abuse Act'. Gezien deze laatste echter gelimiteerd was in zijn toepassingsgebied, werd deze in 1986 al herzien.[581] De Act van 1986 was gericht op de 'confidentiality', 'integrity' en 'availability' van computers en netwerken. De 'Computer Fraud and Abuse Act' werd meermaals aangepast, met name in 1990, 1994, 1996, en in 2001 door de 'USA Patriot Act'. De laatste wijziging dateert van 2008, door de 'Identity Theft Enforcement and Restitution Act'.[582] Concreet bevat

[580] J.R. HERRERA-FLANIGAN, "Cybercrime and jurisdiction in the United States" in B.J. KOOPS en S.W. BRENNER, *Cybercrime and jurisdiction: A global survey*, Cambridge, Cambridge University Press, (313) 314.
[581] J.R. HERRERA-FLANIGAN, "Cybercrime and jurisdiction in the United States" in B.J. KOOPS en S.W. BRENNER, *Cybercrime and jurisdiction: A global survey*, Cambridge, Cambridge University Press, (313) 314.
[582] S.W. BRENNER, "Recent developments in US Internet law" in Y. JEWKES en M. YAR, *Handbook of Internet Crime*, Oregon, Willan Publishing, 2010, (437) 437.

artikel 18 US Code s.1030 volgende bepalingen, waarvan ook de poging strafbaar is gesteld:[583]

- obtaining national-security information;
- compromising the confidentiality of a computer;
- trespassing in a government computer;
- accessing a computer to defraud and obtain something of value;
- damaging a computer;
- trafficking in passwords;
- threatening to damage a computer.

357. Het bovenstaande kan beschouwd worden als de Amerikaanse basistekst in de strijd tegen cybercriminaliteit. Hiernaast zijn er echter nog andere teksten, die meer specifieke veruitwendigingsvormen van cybercriminaliteit viseren.

1.2 The Child Pornography Protection Act

358. In 1996 heeft het Amerikaanse Congress de 'Child Pornography Protection Act' aangenomen, in de strijd tegen de verspreiding van kinderpornografie op het internet. Op deze manier werd de desbetreffende wetgeving up to date gebracht. Nadien werd de 'Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act', ook wel de 'PROTECT Act' genoemd, boven de doopvont gehouden. Met deze laatste Act werd de 'Child Pornography Protection Act' aangepast. Zo werd onder andere de definitie van kinderpornografie aangepast.[584]

1.3 The Wiretap Act

359. Deze Act kan gebruikt worden tegen hackers die inbreken in computersystemen, waarna ze de controle over het systeem overnemen. De Act, die vervat zit in artikel 18 USC § 2511, verbiedt het opzettelijk onderscheppen van elke tele- en elektronische communicatie.

[583] J.R. HERRERA-FLANIGAN, "Cybercrime and jurisdiction in the United States" in B.J. KOOPS en S.W. BRENNER, *Cybercrime and jurisdiction: A global survey*, Cambridge, Cambridge University Press, (313) 315.
[584] S.W. BRENNER, "Recent developments in US Internet law" in Y. JEWKES en M. YAR, *Handbook of Internet Crime*, Oregon, Willan Publishing, 2010, (437) 449.

Personen die zich schuldig maken aan dergelijke feiten riskeren een maximale gevangenisstraf van vijf jaar en/of een geldboete van 250.000 dollar.[585]

1.4 The Electronic Communications Privacy Act

360. Deze Act, die vervat zit in artikel 18 USC § 2701 en volgende, is ook gericht op inbraakpogingen in een informaticacontext. De Act verbiedt meer bepaald het zich opzettelijk en wederrechtelijk toegang verschaffen tot een computersysteem en de inhoud ervan.[586]

2. BEPALINGEN VAN STRAFPROCESRECHT

361. Uit een handreiking van het Department of Justice blijkt dat de Amerikaanse opsporingsdiensten vergelijkbare mogelijkheden hebben als de Belgische en de Nederlandse opsporingsdiensten. Deze Amerikaanse opsporingsdiensten, die hierna zullen besproken worden, kunnen een netwerkzoeking uitvoeren, evenals Internet Service Providers verplichten hun medewerking te verlenen. Ook de inbeslagname en de doorzoeking van computers is een mogelijkheid voor de opsporingsdiensten. [587] Sinds 2011 heeft het US House of Representatives een nieuwe 'Bill' goedgekeurd, waarbij een dataretentie wordt voorzien van twaalf maanden. [588]De Verenigde Staten hebben in dat kader eenzelfde termijn voorhanden, als deze die in België werd voorzien, maar waarvoor nog steeds geen uitvoeringsbesluit is uitgevaardigd.

3. CONCLUSIE

362. Hoewel de wettelijke bepalingen een andere vorm aannemen in de Verenigde Staten, zijn de materiële strafbaarstellingen en de bepalingen van het strafprocesrecht in grote lijnen vergelijkbaar met deze uit België en Nederland. De Verenigde Staten hebben dan ook het Cybercrime-Verdrag ondertekent, wat de zekere tendens van uniformisering verklaart.

---

[585] J.R. HERRERA-FLANIGAN, "Cybercrime and jurisdiction in the United States" in B.J. KOOPS en S.W. BRENNER, *Cybercrime and jurisdiction: A global survey*, Cambridge, Cambridge University Press, (313) 315.
[586] J.R. HERRERA-FLANIGAN, "Cybercrime and jurisdiction in the United States" in B.J. KOOPS en S.W. BRENNER, *Cybercrime and jurisdiction: A global survey*, Cambridge, Cambridge University Press, (313) 316.
[587] U.S. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009, 287 p., www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.
[588] http://judiciary.house.gov.

Hoofdstuk 3: De opsporing en de vervolging in de Verenigde Staten

1. INLEIDING

363. In het kader van de opsporing van cybercriminaliteit, heeft de 'U.S. Department of Justice' een handreiking opgesteld omtrent de zoeking in computersystemen, de inbeslagname, en de bewijsvergaring.[589] Het document bevat bepalingen omtrent het doorzoeken en inbeslagnemen van computers zonder, en met, een huiszoekingsbevel. Daarenboven bevat het document tevens bepalingen omtrent de netwerkzoeking en de bewijsvergaring.

2. DE OPSPORINGSINSTANTIES

2.1 Federal Bureau of Investigation (FBI)

2.1.1 Algemeen

364. Op federaal niveau is het FBI de belangrijkste opsporingsdienst aangaande cybercriminaliteit. Het FBI leidt de 'National Cyber Investigative Joint Task Force'. Deze Task Force houdt zich bezig met de aanpak van veruitwendigingsvormen van cybercriminaliteit. Het FBI ondersteunt daarenboven het 'Department of Homeland Security', door bedreigingen en incidenten, met betrekking tot computers en netwerken, te onderzoeken.[590]

365. Binnen het FBI zijn er speciale teams opgericht, Cyber Action Teams genaamd, die zich bezighouden met de aanpak van erg ingewikkelde zaken. Dergelijke teams bestaan uit hoogopgeleide FBI-agenten, analisten en informatica-experten.[591]

[589] U.S. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009, 287 p., http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.
[590] www.fbi.gov.
[591] www.fbi.gov/news/stories/2006/march/cats030606.

366. Het FBI heeft eveneens bijgedragen tot de oprichting van de 'National Cyber-Forensics & Training Alliance'. Reeds in 1997 zag deze organisatie het levenslicht. De National Cyber-Forensics & Training Alliance brengt politiediensten samen met de privésector en de academische wereld. De rol van de organisatie is vooral die van een waarschuwingscentrale. Daarnaast richt de NCFTA zich op de training van manschappen, en dat zowel op nationaal als internationaal vlak.[592]

367. Het FBI maakt tenslotte ook deel uit van de 'Strategic Alliance Cyber Crime Working Group'. Deze werkgroep, die naast het FBI ook instellingen uit Australië, Canada, het Verenigd Koninkrijk en Nieuw-Zeeland als leden heeft, houdt zich bezig met het in kaart brengen van fenomenen van cybercriminaliteit.[593]

2.1.2 Carnivore

368. Het 'Carnivore-systeem' is een programma ontwikkeld door het FBI, en werd operationeel in 1997. Het laat het FBI toe elke Amerikaanse internetprovider af te luisteren, en het dataverkeer te onderscheppen. Het filtert daarenboven niet alleen op de IP-adressen van zenders of ontvangers, maar ook op inhoud. Nadien werd de inhoud door een computersysteem nagegaan, op zoek naar verdachte woorden. Het computersysteem beschikte over een lijst met verdachte woorden, en selecteerde de berichten waarin dergelijke woorden voorkwamen, voor verder onderzoek. Het systeem heeft dan ook heel wat ophef veroorzaakt. In 2005 werd het vervangen door meer commerciële programma's zoals NarusInsight.[594] [595]

2.2 United States Secret Service

369. Net als het FBI, spoort ook de US Secret Service cybercriminaliteit op. De Secret Service focust zich daarbij vooral op identiteitsdiefstallen en computergerelateerde fraude. Hun inbreng aangaande de strijd tegen cybercriminaliteit nam een hoge vlucht, na het ontstaan van de US Patriot Act.[596] Binnen dit kader heeft de Secret Service dan ook de

[592] www.fbi.gov/news/stories/2011/september/cyber_091611.
[593] www.fbi.gov/news/stories/2008/march/cybergroup_031708.
[594] www.pcworld.com/article/119404/stopping_carnivore_doesnt_stop_fbi_surveillance.html.
[595] www.iusmentis.be.
[596] http://www.secretservice.gov/criminal.shtml.

'Electronic crimes Task Forces' opgericht, en heeft de leiding over het 'National Computer Forensic Institute'.[597]

2.3 Homeland Security

370. Ook het Department of Homeland Security bindt de strijd aan tegen cybercriminaliteit. Het departement werkt in dit kader samen met zowel publieke als private partners. Waar het FBI en de Secret Service zich meer richten op het opsporen van cybercriminaliteit, gaat Homeland security zich meer richten op 'Cybersecurity'. Hun grootste opdracht bestaat er dan ook uit de bevolking bewust te maken van de problematiek van cybercriminaliteit.[598]

3. DE VERVOLGING VAN CYBERCRIMINALITEIT

371. In de Verenigde Staten geschiedt de vervolging van misdrijven door de 'Offices of the United States Attorneys'. De US Attorneys spelen een vitale rol in de vervolging van cybercriminaliteit. De leden van het departement worden dan ook speciaal opgeleid om aan de uitdagingen die cybercriminaliteit met zich meebrengen, te kunnen voldoen.[599] Uit de meest recente cijfers, die van 2010, blijkt dat er gedurende dat jaar 155 zaken zijn behandeld, waarvan er 145 werden afgehandeld in datzelfde jaar. In 86% van de gevallen leidde dit tot de vervolging, en nadien tot een veroordeling.[600] Een cijfer dat vele malen hoger ligt dan in België, waar we in de cijfers van de parketten vooral veel zondergevolgstellingen zien, eerder dan effectieve vervolgingen.

4. CONCLUSIE

372. De Verenigde Staten hebben, net als Nederland, van cybercriminaliteit een prioriteit gemaakt. Verschillende instanties, zoals het FBI, de Secret Service en Homeland Security, houden zich bezig met de aanpak van cybercriminaliteit. De verschillende instanties die hierboven werden besproken, maken deel uit van de aanpak op federaal niveau. Echter, op het niveau van de deelstaten wordt cybercrime eveneens aangepakt, zij het door lokale afdelingen

[597] http://www.secretservice.gov/criminal.shtml.
[598] http://www.dhs.gov.
[599] http://www.justice.gov.
[600] U.S. Department of Justice, *United States Attorneys' Annual Statistical Report*, 2010, 27. (119)

van deze drie instanties. Dit impliceert dat globaal genomen, er een aanzienlijke groep mensen bezig is met de strijd tegen cybercriminaliteit.

373. Ook bij de Amerikaanse parketten zien we een professionele aanpak. Het aantal zaken die voor de Attorney's komen, leiden in een grote meerderheid van de gevallen tot een effectieve veroordeling. Dit beeld staat in schril contrast met de situatie in België, waar de parketten in het merendeel van de gevallen tot seponeren overgaan.

Hoofdstuk 4: De straftoemeting door de rechter

1. INLEIDING

374. In dit hoofdstuk zal aan de hand van enkele concrete 'cases' nagegaan worden of de wettelijke bepalingen hun weg naar de praktijk hebben gevonden. Met het oog op het scheppen van een beeld omtrent de straftoemeting in de Verenigde Staten, zullen in dit kader vier cases besproken worden, die elk betrekking hebben op verschillende veruitwendigingsvormen van cybercriminaliteit.

2. US VS. JASON ARABO

375. De verdachte, Jason Arabo, had in het jaar 2004 meerdere computersystemen van concurrerende bedrijven gehacked en lamgelegd. Hij had hiervoor de hulp ingeroepen van een minderjarige kompaan. Jason Arabo hoopte hiermee klanten aan te trekken voor zijn eigen website, gezien deze van zijn concurrenten onbeschikbaar waren. De aanvallen op de computersystemen geschiedden door zogenaamde 'Denial of Service attacks', waarmee hij de controle verwierf over de respectievelijke netwerken. Zijn daden werden aan het licht gebracht door een onderzoek van het FBI. In 2006 werd Jason Arabo bestraft met dertig maanden gevangenisstraf en een schadevergoeding van 504.495 dollar. De minderjarige kompaan werd veroordeeld tot vijf jaar gevangenisstraf in een jeugdgevangenis, en een schadevergoeding van 32.000 dollar.[601]

[601] S. ROBINSON, "Busted Hackers and Cybercriminals", *Brighthub* 2010, www.brighthub.com.

3. US VS. KENNETH KWAK

376. In deze zaak betrof het een verdachte, die ongeoorloofd toegang had verworven tot het computersysteem van het 'Department of Education'. De verdachte, die een werknemer was van het departement, verkreeg zo informatie over één van zijn diensthoofden, die hij doorstuurde naar zijn collega's. Kenneth Kwak werd, op grond van 'Illegal Computer Monitering' veroordeeld tot vijf maanden gevangenisstraf, en tot betaling van een schadevergoeding van 40.000 dollar.[602]

4. US VS. JEANSON JAMES ANCETA

377. Deze zaak had betrekking op een verdachte, die via een botnet spam-aanvallen uitvoerde op de computersystemen van de 'US Federal Government for National Defense'. Jeanson James Anceta werd, op grond van 'Botnet Computer Tampering', veroordeeld tot een gevangenisstraf van vijf jaar, en een schadevergoeding van 15.000 dollar.[603]

5. US VS. KENNETH FLURY

378. Deze zaak had betrekking op bankfraude. De verdachte in kwestie had in 2004 geprobeerd Citibank op te lichten door middel van gestolen, en vervalste bankkaarten en PIN-codes. Deze case was zodanig opzienbarend in de Verenigde Staten, dat de Secret Service er zich over gebogen heeft. Kort nadien werd de verdachte dan ook bij de kraag gevat. Kenneth Flury werd in 2006 veroordeeld tot drie jaar gevangenisstraf, en een schadevergoeding van 300.000 dollar, op grond van 'Bank and Credit Card Fraud'.[604]

6. CONCLUSIE

379. Zoals uit bovenstaande cases blijkt, hebben ook de Amerikaanse rechters op succesvolle wijze cybercriminelen kunnen veroordelen op grond van de specifieke incriminaties. Opvallend in dit kader zijn de grote schadevergoedingen die de veroordeelden keer op keer

[602] S. ROBINSON, "Busted Hackers and Cybercriminals", *Brighthub* 2010, www.brighthub.com.
[603] S. ROBINSON, "Busted Hackers and Cybercriminals", *Brighthub* 2010, www.brighthub.com.
[604] S. ROBINSON, "Busted Hackers and Cybercriminals", *Brighthub* 2010, www.brighthub.com.

dienen te betalen. Dergelijke sommen zijn in de Belgische en de Nederlandse rechtspraak tot op vandaag niet terug te vinden. De duur van de gevangenisstraffen is dan weer wel vergelijkbaar met de veroordelingen die in België, en vooral in Nederland, worden uitgesproken.

Hoofdstuk 5: Conclusie

380. De Verenigde Staten zijn al sinds de jaren ’80 op een bewuste manier bezig met de strijd tegen cybercriminaliteit. De strafbaarstellingen en de bepalingen omtrent het strafprocesrecht, komen in grote lijnen overeen met deze die we in België en Nederland kunnen terugvinden. Dit is het gevolg van het feit dat deze drie landen het Cybercrime-Verdrag hebben ondertekend, wat heeft geleid tot een zekere uniformisering van de wettelijke bepalingen. De Verenigde Staten hebben, net als Nederland, een prioriteit gemaakt van de aanpak van cybercriminaliteit. Op het federale niveau zijn er, op een geïntegreerde wijze, verschillende instanties bezig met de aanpak van cybercriminaliteit. De VS heeft daarenboven ook zwaar ingezet op de scholing en vorming van het politiepersoneel. Een opvallend gegeven is de hoge graad van vervolgingen, die worden ingesteld nadat zaken omtrent cybercriminaliteit voor de Amerikaanse parketten komen. In maar liefst 86% van de gevallen kwam het tot een vervolging, een percentage dat vele malen hoger ligt dan in België en Nederland. Wat de straftoemeting betreft kunnen we stellen dat ook de rechters in de VS de bepalingen die voorhanden zijn, op een succesvolle manier weten te gebruiken.

DEEL VIII: Algemene conclusie

381. De maatschappij waar we vandaag met z'n allen deel van uitmaken, kunnen we omschrijven als een digitale maatschappij. De laatste twee decennia zijn gekenmerkt door een aanzienlijke technologische vooruitgang. Alle geledingen van de maatschappij zijn als het ware doordrongen met informatie- en telecommunicatietechnologie. Daarenboven heeft het internet als medium, een steeds centralere rol in ons leven ingenomen. Deze vooruitgang dient zondermeer als een positief gegeven beschouwd te worden. Zowel particulieren, overheden, als bedrijven plukken de vruchten van de opportuniteiten die deze technologie hen biedt.

382. Diezelfde opportuniteiten laten echter ook criminelen niet ongemoeid. Het is een aloud gegeven dat opportuniteiten en criminaliteit hand in hand gaan. De digitale maatschappij heeft daarom ook te kampen met een schaduwzijde. De anonimiteit die het internet biedt, heeft een aanzienlijke aantrekkingskracht op cybercriminelen. Het is een uitgelezen werkterrein voor mensen met minder goede bedoelingen. We zien dan ook dat, sinds de opkomst van het internet, meer en meer misdrijven een transitie beginnen te maken naar deze virtuele wereld. Diezelfde transitie heeft bij vele overheden voor flinke hoofdbrekens gezorgd. Gezien het er alle schijn van heeft dat de digitale evolutie zich, naar de toekomst toe, nog verder door zal trekken, stelt zich de vraag hoe men deze soort van criminaliteit dient aan te pakken. Tevens manifesteren er zich vragen naar de wijze waarop men cybercriminaliteit op een efficiënte wijze kan opsporen en vervolgen. Met deze masterproef werd gepoogd een antwoord op deze prangende vragen te formuleren.

383. Tal van internationale organisaties, zoals de OESO, de VN en de G8 hebben zich reeds over de problematiek van cybercriminaliteit gebogen. Hun respectievelijke aanpak is doorspekt met goede bedoelingen, maar tot spijkerharde bepalingen in de strijd tegen cybercriminaliteit, is het echter niet gekomen. De enige internationale organisatie die wel tot dergelijke bepalingen is gekomen, is de Raad van Europa. In de schoot van deze instantie, werd op 23 november 2001 het Cybercrime-Verdrag boven de doopvont gehouden. Deze datum is een mijlpaal geweest in de strijd tegen cybercriminaliteit. Het is, tot op vandaag, het enige internationale verdrag omtrent dit thema. Het verdrag heeft de krijtlijnen uitgetekend met nieuwe strafbaarstellingen, bepalingen van strafprocesrecht en bepalingen omtrent de rechtsmacht. De grootste verdienste die we het verdrag echter kunnen toeschrijven, is die van de uniformisering. De landen die het verdrag hebben ondertekend, hebben namelijk in grote mate gelijklopende bepalingen in hun rechtsbestel opgenomen.

384. Toch dienen er ook kanttekeningen geplaatst te worden bij het Cybercrime-Verdrag. Initieel was het namelijk de bedoeling om ook bepalingen omtrent racisme en xenofobie in de verdragstekst op te nemen. De Verenigde Staten hebben zich daar destijds sterk tegen verzet, gezien een dergelijk verbod zou indruisen tegen het Eerste Amendement van de Amerikaanse grondwet, dat het recht op vrije meningsuiting waarborgt. Gezien de Raad van Europa de VS als een belangrijke partner beschouwde, werden de bepalingen in kwestie uit de verdragstekst geweerd. Er werd in dit kader dan ook geopteerd voor een 'compromis à la Belge', waarbij de bepalingen omtrent rassenhaat en xenofobie in het aanvullend protocol van 28 januari 2003 werden opgenomen. Op deze manier kon de VS zich aansluiten bij het verdrag, zonder de bepalingen omtrent rassenhaat en xenofobie te hoeven aanvaarden. Het blijft betreurenswaardig dat de Raad van Europa zich van dergelijke constructies heeft moeten bedienen, en het zegt daarenboven veel over de machtsverhoudingen in de hedendaagse wereld. Niettemin dient het Cybercrime-Verdrag als een succes beschouwd te worden, al wordt het stilaan tijd voor een opvolger.

385. Het jaar 2010 had in dat opzicht alles om een nieuwe mijlpaal te worden in de strijd tegen cybercriminaliteit. Onder de vleugels van de VN waren er op dat moment vergevorderde onderhandelingen aan de gang omtrent een nieuwe internationale tekst, aangaande cybercriminaliteit. Op een VN-congres in Brazilië werd er gedurende tien dagen gedebatteerd over het voorstel, maar de onderhandelingen liepen met een sisser af. De Europese Unie, de Verenigde Staten en het Verenigd Koninkrijk zagen de noodzaak van een nieuw wereldwijd verdrag niet in, gezien het Cybercrime-Verdrag, naar hun mening, ruimschoots voldeed. Zij stonden hiermee lijnrecht tegenover China, Rusland, en tal van ontwikkelingslanden.

386. Ook de Europese Unie heeft stappen genomen in de strijd tegen cybercriminaliteit. In dit kader zag het Kaderbesluit 2005/222/JBZ van de Europese Raad over aanvallen op informatiesystemen, het levenslicht. Het kaderbesluit dient gesitueerd te worden binnen de context van het eEurope-actieplan. Het preciseert in zekere zin het Cybercrime-Verdrag van de Raad van Europa, en heeft als doelstelling de samenwerking tussen de justitiële en andere bevoegde instanties van de lidstaten te bevorderen, door middel van harmonisatie van de strafrechtelijke bepalingen. Verder heeft het kaderbesluit het doel de verschillende activiteiten op internationaal niveau, zoals de activiteiten in de schoot van de G8 en de Raad van Europa, verder te ontwikkelen.

387. Wat de Belgische situatie betreft, dienen we vast te stellen dat de Belgische wetgever, wat cybercriminaliteit betreft, lang niet thuis gaf. Waar België in de jaren ’90 blijk gaf van een standvastige wil tot achterophinken, werden in Nederland en de VS reeds wetgevende initiatieven genomen. België heeft geprobeerd de opgelopen achterstand weg te werken met de wet van 28 november 2000 inzake informaticacriminaliteit. Deze wet, die quasi gelijktijdig met het Cybercrime-Verdrag tot stand kwam, heeft nieuwe strafbaarstellingen en bepalingen van strafprocesrecht ingevoerd. De bepalingen van materieel strafrecht zijn gelijklopend met deze voorzien in het Cybercrime-Verdrag. Meer bepaald wordt de valsheid in informatica, het informaticabedrog, de ongeoorloofde toegang en de sabotage strafbaar gesteld. Soortgelijke incriminaties kunnen we eveneens in het Nederlandse en Amerikaanse rechtsbestel terugvinden. Wat het strafprocesrecht betreft, bracht de wet van 28 november 2000 vernieuwingen in de vorm van het databeslag, de netwerkzoeking en de medewerkingsverplichting. Verder werden de artikelen 90ter, 90quater en 90septies van het Wetboek van Strafvordering van aanvullingen voorzien. Deze bepalingen van strafprocesrecht kunnen we, met dank aan de uniformiserende werking van het Cybercrime-Verdrag, eveneens terugvinden in Nederland en de VS. Twaalf jaar na de totstandkoming van de wet van 28 november 2000 kunnen we een positieve balans opmaken. Waar de Belgische rechters zich in de jaren ’90 dienden te behelpen met strafbepalingen die daar terminologisch niet voor geschikt waren, heeft de wet van 28 november 2000 hen van een beter instrumentarium voorzien. Mits enkele aanpassingen, die de wet de afgelopen jaren heeft ondergaan, heeft de wet van 28 november 2000 goed standgehouden. Toch dienen we ook hier een negatieve kanttekening te plaatsen. Het blijft met name betreurenswaardig, dat er nog steeds geen Koninklijk Besluit inzake dataretentie tot stand is gekomen, waarbij de voorwaarden worden vastgesteld waaronder operatoren verkeersgegevens en identificatiegegevens van eindgebruikers dienen te bewaren.

388. Het opsporen van cybercriminaliteit is in België, op federaal niveau, aan de Federal Computer Crime Unit toevertrouwd. De FCCU zag het levenslicht na de wet op de politiehervorming, en wordt sinds 2001 geleid door Luc Beirens. De FCCU kan zich, met de middelen die de wet van 28 november 2000 heeft aangereikt, volledig richten op het opsporen van allerlei soorten cybercriminaliteit. Het hoofddoel van de FCCU heeft, in dit kader, betrekking op aanvallen op kritieke informaticasystemen. De opsporing van cybercriminaliteit loop echter niet altijd van een leien dakje.

389. Ten eerste stelt het medium internet zelf, de rechercheurs voor problemen. Zij dienen met name te opereren in een uitgestrekte wereld, gekenmerkt door de vluchtigheid van gegevens. Dit noopt hen dan ook tot snelle interventies, wat in het kader van cybercriminaliteit niet altijd voor de hand liggend is. Cybercriminaliteit houdt immers geen rekening met landsgrenzen, waardoor de rechercheurs vaak te maken krijgen met grensoverschrijdende zaken. Op dat punt dient dan ook gebruik gemaakt te worden van de systemen van de rechtshulp en de internationale samenwerking, wat de behandeling van een dossier aanzienlijk kan vertragen.

390. Ten tweede ondervindt de FCCU structerele moeilijkheden, welke zijn toe te wijzen aan de manier waarop de Belgische overheid tegen cybercriminaliteit aankijkt. België heeft, in tegenstelling tot Nederland en de VS, van cybercriminaliteit geen grote prioriteit gemaakt. Deze opvatting heeft zich de voorbije jaren dan ook vertaald in een stiefmoederlijke behandeling van de FCCU. Het budget dat de FCCU ter beschikking krijgt, is een peulschil in vergelijking met de twee eerder genoemde landen. Waar landen als de Verenigde Staten en Nederland aanzienlijke financiële middelen uittrekken voor de bestrijding van cybercriminaliteit, dient de FCCU te werken met een minimum aan budget. Ook wat de personeelcapaciteit betreft hinkt de FCCU achterop. Waar de FCCU beschikt over vijfentwintig operationele rechercheurs, zijn er dat in Nederland maar liefst honderd. Ook de vorming en scholing, die volledig intern geschiedt, is in België niet doordacht aangepakt. Nederland en de VS doen het ook op dit punt veel beter. In Nederland heeft men ervoor geopteerd om in te zetten op een breed gespreide deskundigheid, waarbij alle politiemedewerkers een SSR-leergang dienen te volgen. Op deze wijze worden de gespecialiseerde diensten ontlast, zodat deze zich kunnen focussen op de grote zaken van cybercriminaliteit. Ook de Verenigde Staten hebben in dit opzicht een instelling voor vorming en scholing in het leven geroepen. Nederland en de VS hebben daarenboven inspanningen gedaan om een geïntegreerde aanpak te bewerkstelligen. Een voorbeeld daarvan in Nederland is het forensisch laboratorium, waarbinnen een team voor digitale expertise is opgenomen, voor moeilijk gevallen van datarecuperatie. Een ander mooi voorbeeld van die aanpak in Nederland vinden we terug bij het Nationaal Cyber Security Centrum, dat begin dit jaar werd opgericht. Ook de Verenigde Staten hebben, op vergelijkbare wijze als Nederland, geopteerd voor een dergelijke geïntegreerde aanpak.

391. Ten derde zijn er ook nog bemerkingen te maken omtrent het wettelijk kader. Luc Beirens stelt in dit opzicht dat de FCCU voldoende slagkracht heeft, maar wijst er tevens op dat er nog ruimte voor verbetering is. Hij doelt hiermee op de stringente regeling voorzien door de BOM-wet, waardoor de FCCU enigszins gekortwiekt wordt. Luc Beirens is dan ook een voorstander van de versoepeling van de BOM-wet.

392. Het wordt hoog tijd dat bepaalde punten omtrent de werking van de FCCU grondig worden aangepakt. Begin dit jaar had het er alle schijn van dat deze verandering er zou komen. Op dat moment werd België immers geconfronteerd met het Tor-netwerk. De politici sprongen, in de nasleep van de affaire, op de barricades. De FCCU moest en zou meer middelen krijgen om cybercriminaliteit grondig aan te pakken. Na verloop van tijd ging de storm echter liggen, waarna het Tor-netwerk uit de media verdween. Hand in hand met de media-aandacht, verdwenen tevens de goede voornemens en krachtige uitspraken van de politici. De zo verhoopte verandering, kwam er niet. De nood aan veranderingen blijft echter groot, wil de FCCU op een adequate manier dergelijke delicten kunnen opsporen.

393. De vervolging van misdrijven ligt in het Belgische rechtsbestel in handen van het Openbaar Ministerie, dat het monopolie van de strafvordering heeft. Het beleid inzake cybercriminaliteit, werd in dit kader vorm gegeven door een reeks omzendbrieven van het college van Procureurs-generaal. Op deze wijze werden de afgelopen jaren de krijtlijnen van het vervolgingsbeleid van de parketten uitgetekend. Uit de cijfers van de satitistische analisten van het Openbaar Ministerie, kan afgeleid worden dat over een periode van tien jaar het aantal informaticazaken, die voor de parketten bij de rechtbanken van eerste aanleg verschijnen, significant is toegenomen. Al even opmerkelijk is dat het merendeel van de gevallen uitmonden in een seponering van de zaak. In Nederland, en nog meer in de VS, zien we het omgekeerde. Het merendeel van zaken die worden behandeld leiden uiteindelijke tot de vervolging.

394. In het kader van deze masterproef werd ook de rechtspraak omtrent cybercriminaliteit onder de loep genomen, dit zowel voor wat België, Nederland en de Verenigde Staten betreft. Uit de verschillende zaken blijkt dat de rechters op een succesvolle en adequate manier gebruik maken van de bepalingen die ze voorhanden hebben. In elk van de drie landen zijn er al tal van veroordelingen geweest inzake cybercriminaliteit. Opmerkelijk daarbij is dat de gevangenisstraffen en de geldboetes die in Nederland en België worden opgelegd,

betrekkelijk laag liggen. In de Verenigde Staten liggen zowel de vrijheids- als de geldstraffen aanzienlijk hoger.

395. De inspanningen die zowel op internationaal, als Belgische niveau zijn genomen, hebben zeker hun vruchten afgeworpen. Er dient evenwel op gewezen te worden dat dit geen reden mag zijn om op de lauweren te gaan rusten, integendeel. Zowel wat de opsporing als de vervolging betreft, dient er ingegrepen te worden. Zoniet dreigen de opsporings- en vervolgingsinstanties overspoeld te worden door de omvang van cybercriminaliteit. Het ligt in de lijn der verwachtingen dat het internet, en de hieraan gerelateerde technologie, alleen maar aan belang zal toenemen. Hand in hand met deze evolutie, zal ook cybercriminaliteit zich verder ontwikkelen. Het komende decennium zal dan ook, zowel voor wetgevers, opsporingsdiensten als vervolgingsinstanties, belangrijk worden om de impact van cybercriminaliteit in te dijken.

DEEL IX: Bibliografie

BIBLIOGRAFIE

WETGEVING

Europa

Wetgeving sensu stricto

- Kaderbesluit Raad van Europa 2005/222/JBZ, 24 februari 2005 over aanvallen op informaticasystemen, *PB*, 16 maart 2005, Nr. L 69/67.

Voorbereidende documenten

- Report of the European Committee on Crime Problems, 1990, Strasbourg.

- Discussion Paper for Expert's Meeting on Retention of Traffic Data, 6 november 2001, http://ec.europa.eu.

- EU forum on Cybercrime Plenary session, 27 November 2001, Brussels, http://ec.europa.eu.

- Nota Raad 15456/01, betreffende het voorstel van het Spaanse voorzitterschap en initiatief van Europol tot instelling bij Europol van een waarnemingscentrum voor computercriminaliteit, 18 december 2001, 5.

- Commission proposal for a Council framework decision on attacks against information systems, 19 april 2002, http://ec.europa.eu.

- Mededeling Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende de bescherming van kritieke informatie-infrastructuur, 30 maart 2009, Brussel.

België

Wetgeving sensu stricto

- Wet 19 juli 1930 tot oprichting van de Regie van Telegraaf en Telefoon, *B.S.*, 2 augustus 1930.

- Wet 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.*, 27 maart 1991.

- Wet 10 juni 1998 tot wijziging van de Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en -telecommunicatie, *B.S.* 22 september 1998.

- Wet 7 december 1998 tot organisatie van een geïntegreerde politiedienst, *B.S.* 8 januari 1999.

- Wet 7 mei 1999 op de kansspelen, de kansspelinrichtingen en de bescherming van de spelers, *B.S.* 30 december 1999.

- Wet 28 november 2000 inzake informaticacriminaliteit, *B.S.* 3 februari 2001.

- Wet 13 juni 2005 betreffende de elektronische communicatie, *B.S.* 30 juni 2005.

- Wet 15 mei 2006 tot wijziging van de artikelen 259bis, 314bis, 504quater, 550bis en 550 ter van het Strafwetboek, *B.S.* 12 september 2006.

- Wet 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten, *B.S.* 18 juli 2007.

- Wet 28 april 2010 houdende diverse bepalingen, *B.S.* 10 mei 2010.

- K.B. 9 januari 2003 tot uitvoering van de artikelen 46bis, §2, eerste lid, 88bis, §2, eerste en derde lid, en 90quater, §2, derde lid van het Wetboek van Strafvordering en van artikel 109ter, E, §2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.* 10 februari 2003.

Voorbereidende documenten

- Wetsvoorstel tot aanvulling van artikel 2 van de drugswet van 24 februari 1921 met het oog op de invoering van verzwarende omstandigheden in het kader van de handel van hormonale substanties voor menselijk gebruik, *Parl. St.* Senaat 2011-12, nr. 5-1274/1.

- Wetsontwerp inzake informaticacriminaliteit, *Parl. St.* Kamer, Memorie van toelichting, 3 november 1999, nr. 213/001,12-13.

- Verslag namens de Commissie voor de Justitie, *Belgische Senaat*, 28 juni 2000, 2-392/3, p 78.

- Integraal Verslag met vertaald beknopt verslag van de toespraken, *Parl. St*. Kamer 2011-12, nr. criv 53 com, http://www.dekamer.be/doc/CCRI/pdf/53/ic361.pdf.

- Schriftelijke vraag van de heer Bart Tommelein tot de vice-eerste minister en minister van Financiën en Insitutionele Hervormingen omtrent de website Silk Road, *Hand.* Senaat, 2011-12, 30 september 2011, nr. 5, 3296.

Nederland

Wetgeving sensu stricto

- Wet 24 december 1992, *Stb.* 1993, 33.

- Wet 1 juni 2006 inzake computercriminaliteit II, *Stb.* 2006.

TEKSTEN VAN INTERNATIONALE INSTANTIES

- Recommendation Council of Europe No. R (89) 9 adopted by the Committee of Ministers of the Council of Europe, 13 september 1989, concerning Computer-Related Crime.

- Recommendation concerning guidelines for the security of information systems, 26 november 1992, www.oecd.org.

- Statement by attorney general Janet Reno on the meeting of justice and interior minister of the eight, 10 december 1997, www.fondazionefalcone.it.

- G8 Conference on High-Tech Crime, 22-24 May 2001, Tokyo, www.statewatch.org.

- Convention on Cybercrime Council of Europe ETS no. 185, 2001. Budapest.

- Explanatory report on the Convention on Cybercrime Council of Europe ETS no. 185, 16 december 2001.

- Additional Protocol to the Convention on Cybercrime Council of Europe ETS no. 189, 2003, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg.

- Report of the Working group on Internet Governance, juni 2005, www.wgig.org.

- G8 Justice and Home Affairs Ministers' Declaration on The Fight Against Piracy, 30 mei 2009, Rome, www.canadainternational.gc.ca.

- Working paper of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice (22 januari 2010), *UN Doc.* A/CONF.213/9 (2009), www.unodc.org.

- Background documents of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice (23 maart 2010), *UN Doc.* A/CONF.213 /IE/7, www.cybercrimelaw.net.

- G8 Preparatory Plans for the 2011 G8 Deauville Summit, 26-27 mei 2011, Deauville, www.g8.utoronto.ca.

- G8 Final Declaration concerning Internet, 26 mei 2011, Deauville, www.g7.utoronto.ca.

OMZENDBRIEVEN COLLEGE PROCUREURS-GENERAAL

- Omzendbrief van het college van Procureurs-generaal 1 oktober 1998 betreffende de wet van 10 juni 1998 tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van prive-communicatie en –telecommunicatie, nr. COL 13/98, www.om-mp.be/extern/getfile.php?pname=3319355.PDF.

- Omzendbrief van het College van Procureurs-generaal 16 april 1999 betreffende de ministeriële richtlijn van 16 maart 1999 tot regeling van de samenwerking, coördinatie en taakverdeling tussen de lokale politie en de federale politie inzake de opdrachten van de gerechtelijke politie, nr. COL 6/99.

- Omzendbrief van het College van Procureurs-generaal 3 juni 1999, betreffende de ministeriële richtlijn houdende het opsporings- en vervolgingsbeleid betreffende mensenhandel en kinderpornografie, nr. COL 12/99, www.om-mp.be/extern/getfile.php?p_name=3318569.PDF.

- Omzendbrief van het college van Procureurs-generaal 14 februari 2002 betreffende de wet inzake informaticacriminaliteit, nr. COL 1/2002, www.om-mp.be/omzendbrief/4017270/omzendbrieven_2002.html.

- Omzendbrief van het college van Procureurs-generaal 7 maart 2002 betreffende de regeling van de taakverdeling, de samenwerking, de coordinatie en de integratie tussen de lokale en de federale politie inzake de opdrachten van gerechtelijke politie, nr. COL 2/2002, www.om-mp.be/omzendbrief/4017270/omzendbrieven_2002.html.

- Omzendbrief van het college van Procureurs-generaal 9 april 2004 betreffende de wet van 7 mei 1999 op de kansspelen, de kansspelinrichtingen en de bescherming van de spelers, nr. COL 8/2004, www.om-mp.be/omzendbrief/4016876/omzendbrieven_2004.html.

- Omzendbrief van het college van Procureurs-generaal 30 april 2004 betreffende het opsporings- en vervolgingsbeleid betreffende mensenhandel – Aanpassing van de richtlijn van de minister van Justitie, nr. COL 10/2004, www.om-mp.be/extern/getfile.php?p_name=3447098.PDF.

- Omzendbrief van het college van Procureurs-generaal betreffende de wet inzake de informaticacriminaliteit- Addendum aan de §§ 58 en 59 van de omzendbrief nr. COL 1/2002, nr. COL 16/2004, www.om-mp.be/omzendbrief/4016876/omzendbrieven_2004.html.

- Omzendbrief van het college van Procureurs-generaal 24 februari 2006 betreffende de kansspelen en de clandestiene inrichtingen, nr. COL 2/2006, www.om-mp.be/omzendbrief/4017068/omzendbrieven_2006.html.

- Omzendbrief van het college van Procureurs-generaal 21 maart 2006 betreffende racisme en xenofobie, nr. COL 6/2006, www.om-mp.be/omzendbrief/4017068/omzendbrieven_2006.html.

- Omzendbrief van het college van Procureurs-generaal 19 februari 2009 betreffende de toepassing van de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten, nr. COL 2/2009, www.om-mp.be/omzendbrief/4123047/omzendbrieven_2009.html.

- Omzendbrief van het college van Procureurs-generaal 18 juni 2009 als addendum aan de gemeenschappelijke omzendbrief van de minister van Justitie en het college van Procureurs-generaal 5/2002 betreffende het federaal parket - Modaliteiten van samenwerking tussen het federaal parket en de centrale directies van de algemene directie van de gerechtelijke politie van de federale politie, nr. COL 9/2009, http://www.om-mp.be/omzendbrief/4123047/omzendbrieven_2009.html.

- Omzendbrief van het college van Procureurs-generaal 17 juli 2009 betreffende de Telecommunicatierichtlijn inzake het opsporings- en vervolgingsbeleid betreffende inbreuken op de medewerkingsverplichtingen vervat in de artikelen 46bis § 2, 88bis § 2 en 90 quater § 2 van het wetboek van strafvordering, nr. COL 14/2009, www.om-mp.be/omzendbrief/4123047/omzendbrieven_2009.html.

- Omzendbrief van het college van Procureurs-generaal 31 december 2010 betreffende de wijzigingen die door de wet van 28 april 2010 houdende diverse bepalingen werden aangebracht aan de wet van 15 mei 2007 betreffende de bestraffing van namaak en piraterij van intellectuele eigendomsrechten, nr. COL 23/2010, www.om-mp.be/omzendbrief/4124639/omzendbrieven_2010.html.

JAARVERSLAGEN

- Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Vijfde Activiteitenverslag 2006, www.polfed-fedpol.be/pub/rapport_activites/rapports_act_nl.php.

- Directie DJF-Ecofin, Federale Gerechtelijke Politie, Directie Economische en Financiële Criminaliteit: Jaarverslag 2010, www.polfedfedpol.be/pub/rapport_activites/rapports_act_nl.php.

- U.S. Department of Justice, *United States Attorneys' Annual Statistical Report*, 2010, 119 p.

RECHTSPRAAK

België

- Antwerpen, 7 oktober 2003, *Computerr.* 2004, 85
- Antwerpen 10 september 2008, *NC* 2009, 328.
- Rb. Brussel 8 november 1990, *Computerrecht*, 1991, 31-32.
- Corr. Eupen 15 december 2003, *Computerr.* 2004, 129 en *RDTI* 2004, 61, noot O. LEROUX.
- Corr. Eupen 15 december 2003, www.internet-observatory.be, noot H. GRAUX.
- Corr Hasselt 21 januari 2004, *Computerr* 2004, 130, noot H. GRAUX.
- Corr. Dendermonde 28 november 2005, *RABG* 2007, 427-432.
- Corr. Dendermonde 14 mei 2007, *T. Strafr*. 2007, 403.
- Corr. Dendermonde 25 mei 2007, *TGR-TWVR* 2007, 351-354.
- Corr. Brussel 8 januari 2008, *JT* 2008, 337-338, noot A. LEROY.
- Corr. Brussel 10 januari 2008, *T. Strafr.* 2008, 149.
- Rb. Dendermonde 29 augustus 2008, www.juridat.be, noot.
- Rb. Dendermonde 14 november 2008, *Computerr.* 2009, 74-76, noot L. DAUWE.
- Corr. Dendermonde 2 augustus 2009, www.juridat.be, gewijzigd door Gent 30 juni 2010, www.juridat.be, vernietigd door Cass. 18 januari 2011, www.juridat.be.

Nederland

- Arnhem 21 november 2006, www.rechtspraak.nl.

- Rb. Utrecht 8 december 2010, www.rechtspraak.nl.

- 's-Gravenhage 23 maart 2012, www.rechtspraak.nl.

RECHTSLEER

Handboeken

- BEIRENS, L., *Informatiefiche inzake de organisatie en werking van de Federal Computer Crime Unit (FCCU) en de Regional Computer Crime Units (RCCU)*, Brussel, 2007, 12 p.

- CLEIREN, C.P.M., en NIJBOER, J.F., *Strafrecht: tekst en commentaar*, Deventer, Kluwer, 2008, 1135 p.

- CLOUGH, J., *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, 449 p.

- DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 214 p.

- GIBSON, W., *Neuromancer*, Vancouver, Harper Collins Paperback, 1995. 320 p.

- HAFNER, K. en M. LYON, M., *Where wizards stay up late: The origins of the internet*, New York, Simon & Schuster, 1998, 304 p.

- HANCE O., *Business op Internet volgens de wet*, Brussel, Mcgraw-hill education, 1996, 471 p.

- Internet Services Providers Association, *Market Survey N°50 - Q4 2011*, Brussel, 2012, www.ispa.be.

- JEWKES, Y. en YAR, M., *Handbook of internet crime*, Devon, Willan Publishing, 2010, 654 p.

- KASPERSEN, H.W.K. *Schriftelijke leergang Nieuwe Telecomwet*, Hilversum, Broadcast Press, 2004, http://pubs.cli.vu/pub168.php.

- KÖHLER, M. en ARNDT, *Recht des Internet*, Heidelberg, Müller Verlag, 2000, 164 p.

- KSHETRI, N., *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, Londen, Springer, 2010, 251 p.

- LAUREYS, T., *Informaticacriminaliteit*, Gent, Mys en Breesch, 2001, 117 p.

- MCGUIRE, M., *Hypercrime: The New Geometry of Harm*, New York, Routledge-Cavendish, 2007, 375 p.

- Nationaal Cyber Security Centrum, *Cybercrime: van herkenning tot aangifte*, Den Haag, 2012, 140 p.

- Nationaal Instituut voor de Statistiek, *Digitale (r)evolutie in België – anno 2010* (persbericht), Brussel, 2011, http://statbel.fgov.be/nl/binaries/ict2010-nl_tcm325-117754.pdf, 6 p.

- OESO, *Computer viruses and Other Malicious Software: A Threat to the Internet Economy*, 2009, 244 p.

- ROBINSON, S., "Busted Hackers and Cybercriminals", *Brighthub* 2010, www.brighthub.com

- STERLING, B., *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Harmondsworth, Penguin, 1994, 336 p.

- U.S. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009, 287 p., www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

- VAN DEN WYNGAERT, C., *Strafrecht en strafprocesrecht in hoofdlijnen*, II, Antwerpen, Maklu, 2009,1286 p.

- VAN EECKE, P., *Criminaliteit in Cyberspace: Misdrijven, hun opsporing en vervolging op de informatiesnelweg*, Gent, Mys en Breesch, 1997, 121 p.

- VERMEULEN, G., *Wederzijdse rechtshulp in strafzaken in de Europese Unie: naar een volwaardige eigen rechtshulpruimte voor de Lid-Staten?*, Antwerpen, Maklu, 1999, 635 p.

- WESTBY, J. R., *International Guide to Combating Cybercrime*, Chicago, American Bar Association, 2003, 230 p.

- YAR, M., *Cybercrime and society*, Londen, Sage Publications ltd, 2006, 185 p.

Bijdragen in verzamelwerken

- BRENNER, S.W., "Recent developments in US Internet law" in Y. JEWKES en M. YAR, *Handbook of Internet Crime*, Oregon, Willan Publishing, 2010, 437-465.

- DEBAETS, A., DEENE, J. en SENEL, N., "Cybercriminaliteit", in G. VERMEULEN, *Aspecten van Europees materieel strafrecht*, Antwerpen, Maklu-Apeldoorn, 2002, 381- 440.

- DE HERT, P. en LICHTENSTEIN, G., "Informaticacriminaliteit en het formeel strafrecht", in *CBR Jaarboek* 2002-2003, Antwerpen, Maklu, 2003. 345-420.

- SPRUYT, B., "Computers op de strafbank" in B. DE SCHUTTER, *Informaticacriminaliteit*, Kluwer, Antwerpen-Deventer, 1987, 232 ev.

- FRANKEN, H. en KASPERSEN, H.W.K., "Strafrecht en opsporing in computernetwerken", in H. FRANKEN, H.W.K. KASPERSEN en A.H. DE WILD, *Recht en computer*, Deventer, Kluwer, 2004, 385-454.

- HERRERA-FLANIGAN, J.R., "Cybercrime and jurisdiction in the United States" in KOOPS B.J. en S.W. BRENNER, *Cybercrime and jurisdiction: A global survey*, Cambridge, Cambridge University Press, 313-325.

- KLEVE, P., DE MULDER, R.V. en VAN NOORTWIJK, C., "ICT Criminaliteit", in E.R. MULLER, J.P. VAN DER LEUN, L.M. MOERINGS en P.J.V. VAN CALSTER, *Criminaliteit: criminaliteit en criminaliteitsbestrijding in Nederland*, Alphen aan den Rijn, Kluwer, 2010, 259-287.

- VANSTEENHUYSE, S. en T'JONCK, P., "Cybercriminaliteit en privacy", in G. VERMEULEN, *Privacy en strafrecht: Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu-Apeldoorn, 2007, 433-471.

Tijdschriften

- BEIRENS, B., "Op zoek naar criminele bits, digitaal rechercheren", *Politeia* 1998, 9-12.

- BRUINS, A., "Law and order in cyberspace", *Mr. Magazine* 2010, 28-35.

- DE HERT, P. en LICHTENSTEIN, G., "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", *Vigiles* 2004-05, 153-169.

- DE CORTE, R., "ReDaTtacK krijgt deksel op de neus", Juristenkrant 2001, 5-7.

- DE SCHUTTER, B., "Het Belgische Bistel-syndroom", *Computerr.* 1991, 164-166.

- DUMORTIER, E.J., "Het auteursrecht spoelt weg door het elektronische vergiet. Enige gedachten over de naderende crisis van het auteursrecht", *Computerr.* 1994, 109-113.

- DUMORTIER, J., VAN OUDENHOVE, B. en VAN EECKE, P., "De nieuwe Belgische wetgeving inzake informaticacriminaliteit", *Vigiles* 2001, 44-62.

- DUNNE, R.L., "Deterring unauthorized access to computers: controlling behavior in cyberspace through a contract paradigm*", Jurimetrics* 1994, 1-15.

- EVRARD, S., "La loi du 28 novembre 2000 relative à la criminalité informatique, *J.T.* 2001, 241 245.

- GOOSSENS, F., "Wijzigingen in het Belgisch Strafwetboek inzake informaticacriminaliteit", *TVW* 2006, 466-467.

- GRAUX, H., "Cybercrimeverdrag van de Raad van Europa", *ICRI* 2001, www.internet-observatory.be.

- GRAUX, H., "Wet inzake informaticacriminaliteit.", *ICRI* 2001, www.internet-observatory.be.

- GRAUX, H., "Aanvullend protocol bij het Cybercrimeverdrag van de Raad van Europa", *ICRI* 2003, www.internet-observatory.be.

- HARLEY, B., "A global Convention on Cybercrime?", *The Columbia Science and Technology Law review* 23 maart 2010, www.stlr.org.

- KASPERSEN, H.W.K., "De Wet computercriminaliteit is er- nu de boeven nog", *Computerr.* 1993, 134-145.

- KASPERSEN, H.W.K., "Voortgang van het Cybercrimeverdrag", *Computerr.* 2001, 105-106.

- KEUSTERMANS, J. en DE MAERE, T., "Tien jaar wet informaticacriminaliteit", *RW* 2010, 562-568.

- KEUSTERMANS, J. en MOLS, F. "De wet van 28 november 2000 inzake informaticacriminaliteit: een eerste overzicht", *R.W.* 2001-2002, 721-732.

- KOOPS, B.J. en SCHELLEKENS, M.H.M., "Computercriminaliteit II: de boeven zijn er – nu de wet weer", *Nederlands Juristenblad* 1999, 1764- 1772.

- KOOPS, B.J., "Tijd voor Computercriminaliteit III", *Nederlands Juristenblad* 2010, 2461-2466.

- KUITENBROUWER, F., "Verdrag crime in cyberspace", *Computerr.* 2000, 116-117.

- MASTERS, G., "Global cybercrime treaty rejected at U.N.", *SC Magazine* 23 april 2010, www.scmagazine.com.

- Openbaar Ministerie, "Intensief samenwerken tegen de ondermijnende en georganiseerde criminaliteit: aanpak cybercrime", *Twee weten meer dan één* 2012, 12-14.

- PAYE, J., "La loi relative à la criminalité informatique", *Journ. Proc.* 2001, 13-15.

- RIMM, M., "Marketing Pornography on the information Superhighway", *Georgetown Law Journal* 1995, 1849-1934.

- SCHUIJERS, M., en JONGMAN, R., "Speciale uitgave Team High Tech Crime/ Team Bestrijding Kinderporno en Kindersekstoerisme", *KPLD Magazine* 2012, 1-16.

- SENNESAEL, V., "National Computer Crime Unit: digitale flikken", *Computer Magazine* 2000, 73-75

- STOL, W.P., VAN TREECK, R.J., en VAN DER VEN, A.E.B.M., "Criminaliteit met ICT", *Modus* 2000, 8-13.

- TAEYMANS, M., "De wet informaticacriminaliteit in werking getreden", *Computerr.* 2001, 103-104.

- VAN LINTHOUT, P. en KERKHOFS, J., "Internetrecherche: informaticatap en netwerkzoeking, licht aan het einde van de tunnel", *T. Strafr*. 2008, 79-95.

- VAN ROY, B., "Wijzigingen aan de Belgische bepalingen inzake informaticacriminaliteit", *Computerr.* 2006, 314-316.

- VERBIEST, T. en DERVAUX, I.,"La criminalité informatique dans tous ses états", *T.B.H.* 2002, 607-613.

- VERMAAS, P., "High Tech Crime", *Openbaar Ministerie: Opportuun* 2008, 20-23.

KRANTENARTIKELS

- BIESEMANS, J., "G8-landen vergaderen over cybermisdaad", *ZDNet België* 15 mei 2000, www.zdnet.be.

- CLERIX, K., "Gemiddeld 100 tot 200 cybercrime-incidenten per maand in België", *MO* 17 november 2010, www.mo.be.

- DECKMYN, D., "Het cyberleger van Assange", *De Standaard* 12 december 2010, www.destandaard.be.

- DECKMYN, D.,"Speeltuin van wapenhandelaars en drugsdealers", *De Standaard* 4 maart 2012, 16-19.

- DECKMYN, D., "De meerderheid wil gewoon kunnen facebooken", *De Standaard* 5 maart 2012, 6-7.

- ERMERT, M., "Konkurrenz für Cybercrime-Konvention des Europarates", *Heise online* 18 maart 2010, www.heise.de.

- GEUKENS, S., "Eu-Commissie start centrum tegen cybercrime", De Morgen 28 maart 2012, www.demorgen.be.

- HIJINK, M., "De politie mag een beetje terughacken", *NRC Handelsblad* 29 oktober 2010, www.nrc.nl.

- LAGAST, C., "Vlaamse kinderverkrachter opgepakt na Nederlandse undercover-reportage", *De Standaard* 12 februari 2012, www.destandaard.be.

- MURPHY, P., "Remote search and the invisible elephant", ZDNet 28 januari 2009, www.zdnet.com.

- STIENNON, R., "Cyber crime is not bigger than illegal drug trade", *ZDNet* 19 september 2007, www.zdnet.com.

- VAN DEN BROUCKE, B., "Kritiek over werkgever op Facebook reden tot ontslag", *Het Nieuwsblad* 17 november 2011, www.nieuwsblad.be.

- VAN DER VEN, M., "Cybercriminaliteit maakt 3 Belgische slachtoffers per minuut", *De Tijd* 26 september 2011, www.tijd.be.

- VAN EECKE, P.,"COLUMN. Criminaliteit in cyberspace", *De Standaard Online* 26 november 2001, www.standaard.be.

- VAN MILTENBURG, O., "KLPD gaat aantal digitale rechercheurs verdubbelen", *Volkskrant* 3 januari 2012, www.volkskrant.nl.

- X., "Computers crashen wereldwijd door I Love You-virus", *Het Belang van Limburg* 5 mei 2000, www.hbvl.be.

- X., "Verdachte maker 'I Love You'-virus niet vervolgd", *Webwereld* 21 augustus 2000, www. webwereld.nl.

- X., "Cybercrime treaty raises privacy concerns", *ZDNet* 13 oktober 2000, www.zdnet.com.

- X., "Den Haag krijgt europees cybercrimecentrum", De Stentor 28 maart 2012, www.destentor.nl.

- X. “Aantal gerechtelijke arrondissementen daalt naar twaalf”, *Knack* 17 april 2012, www.knack.be.

INTERNETBRONNEN

- http://www.aitglobal.com/orgsite/events/InfoSec2001/un_infosec_2001.htm.
- http://www.bipt.be/nl/21/ShowContent/434/Algemene_voorstelling/Algemene_presentatie.aspx.
- https://www.cert.be/citizen/nl.
- http://www.coe.int.
- http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.
- http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=17/04/2012&CL=ENG.
- http://cwisdb.kuleuven.be/pisa/nl/juridisch/crack.htm.
- http://www.cybercrimelaw.net/OECD.html.
- http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.
- http://www.dhs.gov.
- http://www.enisa.europa.eu/media/press-releases/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011.
- http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1239&format=HTML&aged=0&language=NL&guiLanguage=en.

- http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827.
- https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417.
- http://www.g8.utoronto.ca.
- www.ispa.be.
- http://issat.dcaf.ch/Home/Community-of-Practice/Blogs/INPROL/UNODC-Study-on-Cybercrime.
- www.iusmentis.be.
- http://judiciary.house.gov.
- http://www.justice.gov.
- www.fbi.gov.
- http://www.oecd.org.
- http://oerlemansblog.weblog.leidenuniv.nl/2010/11/05/nieuw-voorstel-voor-een-europese-richtli.
- http://www.om-mp.be/omzendbrieven.html.
- http://www.om-mp.be/sa/jstat2010/n/home.html.
- http://www.om-mp.be/sa/start/n/home.html.
- www.pcworld.com/article/119404/stopping_carnivore_doesnt_stop_fbi_surveillance.html.
- http://www.polfed-fedpol.be/org/org_dgj_FCCU_RCCU_nl.php.

- http://www.polfed-fedpol.be/pub/pdf/NVP2012-2015.pdf.
- http://profs.sci.univr.it/~giaco/download/Watermarking-Obfuscation/cybercrime%20classification.pdf.
- http://pubs.cli.vu/pub168.php.
- http://www.secretservice.gov.
- http://www.security.nl/artikel/38404/1/Symantec%3A_Cybercrime_evenaart_drugshandel.html.
- http://www.slideshare.net/LucBeirens/20120329-infosecurity-bru.
- http://www.spamsquad.be/nl/misc/about.html.
- http://statbel.fgov.be/nl/statistieken/cijfers/arbeid_leven/ict/.
- http://www.security.nl/artikel/2883/1/Europol_krijgt_waarnemingscentrum_voor_hightech criminaliteit.html.
- http://stefaandeclerck.be/files/pdf/Cybercrime_nota_conformiteit.pdf.
- http://www.stefaandeclerck.be/nl/dataretentie/941.
- http://stefaandeclerck.be/files/pdf/dataretentie_KB.pdf.
- http://stefaandeclerck.be/files/pdf/wet_dataretentie.pdf.
- http://www.unodc.org/cybercrime-study/.
- http://www.unodc.org/unodc/en/frontpage/2012/January/unodc-chief-announces-a-comprehensive-study-on-cybercrime.html.

- http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/.
- https://w2.eff.org/Net_culture/net.history.txt.
- http://www.w3.org/.
- http://www.whitehouse.gov/the-press-office/2011/11/28/joint-statement-us-eu-summit.

DEEL X: Bijlagen

Interview met Luc Beirens, hoofd van de Federal Computer Crime Unit, afgenomen op 18 april 2012.

"In welke mate is de Belgische wetgeving aangepast aan de realiteit?"

Als we naar het materieel strafrecht kijken denk ik dat we vrij veel zaken dekken. Natuurlijk zijn er hier en daar wat zaken die afhankelijk zijn van wat de wetgever zelf wil. In Frankrijk bijvoorbeeld, heb je happy slapping, of websites die filmpjes tonen van moorden. Dit heeft met cybercrime op zich niet zoveel te maken, maar dat zijn zaken die er toch in zekere zin aan verbonden zijn. Dat heeft dan betrekking op de randfenomenen, met internet als publicatiemiddel. Onze mogelijkheden wat de opsporing betreft worden wel enigszins beperkt door de strenge regeling in de BOM-wet. De mogelijkheid om te infiltreren bestaat, maar is wel verbonden aan allerlei voorwaarden. Het probleem met de huidige BOM-wet en de opsporingsmethodes is dat men deze moet gaan rechtvaardigen, maar dan moet je wel elementen hebben. Vaak moet je dan wel reeds elementen kunnen vinden, vooraleer je kan overgaan tot toepassing van de bijzondere opsporingsmethoden. Bijvoorbeeld op chatkanalen meelezen of meeluisteren is toegestaan, maar zelf iets typen of zeggen niet, want dat is dan infiltratie. Als je dan op chats waar kinderen opzitten niet mag meedoen, kan je ook niet zien wie die kinderen eventueel wil benaderen. We zijn in dat opzicht wat gekortwiekt. We mogen eigenlijk niet heel veel. Begrijp me niet verkeerd, ik begrijp de beweegredenen waarom dit niet zomaar toegelaten is. We moeten in de opsporing de middelen gebruiken die wettelijk zijn voorzien, met inachtneming van de grondrechten, de privacy, de bescherming van de woning en de bescherming voorzien in de wet op de elektronische communicatie van 2005. Voor alles wat daar tegen ingaat moet je dus machtigingen krijgen van de onderzoeksrechter of de procureur.

"Hoe verloopt een onderzoek dan concreet? Wat is de rol van het ecops loket?"

Ecops is duidelijk maar een meldpunt, de meeste zaken, zoals gewone misdrijven starten bij een klacht, waarbij de onderzoeksrechter ons vertelt wat te doen. Ofwel komt er dus een klacht, ofwel starten we zelf als we iets opmerken. Ecops is natuurlijk één van de startpunten, maar blijft erg beperkt voor ons werk.

"Wat zijn de grootste hindernissen waar jullie mee te maken krijgen gedurende de opsporing?"

Als je kijkt naar het rechtskader dan zit het grootste probleem in het internationaal aspect. Van de 100 dossiers gaan er zeker 95 zijn waarbij we de grens moeten oversteken. In de meeste gevallen zitten de dader en het slachtoffer niet in hetzelfde land, en in het geval dat dit wel zo is, zitten er vaak systemen tussen waarvan de sporen leiden naar het buitenland. Je zit quasi onmiddellijk in een behoefte om sporen in het buitenland te gaan onderzoeken.

"Werken jullie dan samen met buitenlandse Computer Crime Units?"

Jazeker, wij hebben internationale samenwerking via instrumenten als rogatoire commissies. Maar ook recenter zijn er initiatieven voor joint-investigation teams waarbij informatie kan uitgewisseld worden van het ene dossier naar het andere. Het intermezzo waar we eigenlijk het meest mee werken zijn rechtshulpverzoeken. Maar het nadeel daaraan is dat het grote vertragingen meebrengt in het dossier en je kan niet vlot gaan uitwisselen met uw collega's. Het is echter niet aan ons om te gaan kiezen met welke eenheid we gaan samenwerken, het is het land zelf dat bepaalt welke eenheid daar wordt opgezet. Het is wel zo dat er in elk land een 24u permanentiepunt aangeduid is. Als er zeer dringende gevallen zijn kunnen wij contact opnemen met zo'n permanentiepunt en dan wordt het dossier op die manier opgestart. In de meeste gevallen is dat opstarten het feit dat er gegevens bewaard worden ofwel dat we direct informatie geven, waardoor er in het land in kwestie ook een dossier gestart wordt. En dan is het aan de magistraten wat ze concreet kunnen gaan opzetten van samenwerking en welke gegevens het ene land nodig heeft van het andere.

"Met welke inbreuken krijgen jullie het vaakst te maken?"

Het is zo dat we domeinen afbakenen. Wij, als FCCU, maken deel uit van de directie financieel-economische criminaliteit. Normaal gezien, als autonome dienst, hebben wij geen autonome opsporingsbevoegdheid. Dat wil zeggen dat de mensen normaal bij de lokale politie gaan om een klacht neer te leggen, waarna een dossier wordt opgestart. De lokale politie gaat voor beperkte lokale misdrijven hun lokale recherche inschakelen. Eens dat dit arrondissement overstijgend is gaat dat naar de federale recherche. De federale gerechtelijke politie is dan weer op twee niveaus opgesplitst, waarbij de centrale diensten ondersteuning geven aan de arrondissementele diensten. Ofwel worden de dossiers gedraaid door de lokale politie, ofwel door arrondissementele diensten van de federale gerechtelijke politie, waarbij de centrale diensten maar in steun komen. Nu zijn er uitzonderingen op dat principe, en die zitten

allemaal in de directie financieel-economische misdrijven. Hier vertrekken we vanuit het principe, wettelijk voorzien, van de georganiseerde financiële criminaliteit. Daar is dus een speciale dienst binnen onze directie voor. Dan heb je ook nog de anti-corruptie dienst, en daarnaast dan de Federal Computer Crime Unit. Concreet wordt er tussen de federale politie en het FCCU afspraken gemaakt hoe we gaan samenwerken bij aanvallen op grote kritieke systemen. Als de federaal procureur beslist dat een dossier gedraaid wordt door het federaal parket, als ze m.a.w. een zaak federaliseren, dan kan de federaal procureur de FCCU aanduiden als opsporende eenheid. Zo draaien we in feite wel een autonoom dossier, wat eigenlijk een uitzondering is op het wetgevend model. Dat is ook noodzakelijk gebleken, omdat je in dergelijke dossiers vaak met sporen zit in eigen land, verspreid over verschillende arrondissementen, maar eveneens met internationaal verspreide sporen. Bijkomend heb je dan het aspect van de specialisatie voor zo'n complexe dossiers, die niet zo verspreid zit binnen de politie. We hebben dan wel 25 Regionale Computer Crime Units met specialisten, maar als je maar af en toe in contact komt met dergelijke vormen van criminaliteit dan heb je natuurlijk minder ervaring. Als ik dan spreek over de criminaliteit waar wij ons met de Federal Computer Crime Unit mee bezig houden, gaat dat over hacking van zeer grote bedrijven die deel uitmaken van de kritieke infrastructuur. Indien deze zouden platgelegd worden, dan krijg je economische problemen in het land. Dus telkens wanneer zo'n dossier zich aanbiedt gaat de FCCU dat afchecken met het federaal parket, met de vraag of er wordt gefederaliseerd of indien er enkel wordt gecoördineerd. Ofwel behandelen we het dossier dan autonoom, ofwel geven we ondersteuning aan de mensen op het terrein. De vormen van cybercriminaliteit die het meest worden geregistreerd in de databanken van de politie zijn vooral misbruiken van kredietkaarten. Dat is de hoofdmoot van wat geregistreerd wordt. Daarnaast hebben we ook zaken die onder andere te maken hebben met hackingen van internetaccounts, hotmail e.d.. We hebben echter maar een beperkt aantal gevallen per jaar van bedrijven die het slachtoffer worden van hacking en daar een klacht voor neerleggen. Zeer grote bedrijven zijn dan wel uitzonderlijk, toch hebben we enkele van die dossiers. In zulke gevallen zie je dan ook meteen het internationale aspect weer opduiken, waarbij we niet enkel in België onderzoeken moeten doen, maar ook moeten samenwerken met politiediensten uit andere landen, omdat die bedrijven multinationals zijn. Hun infrastructuur is dan ook verspreid over Europa, en zelfs wereldwijd. Wat wij in het recente verleden gedaan hebben, sinds 2007, was focussen op al wat e-banking misdrijven betreft. Het is dan niet zozeer de bank die hier slachtoffer van wordt, maar meer de eindgebruiker, waarbij cybercriminelen kunnen binnendringen tijdens de eigenlijke transactie. Het betreft dan bijvoorbeeld zaken omtrent phishing-websites, maar nog

voorkomend zijn de zaken waarbij de eindgebruiker wordt geïnfecteerd waardoor zijn pc in een botnet komt te staan. Dat botnet gaat dan instructies geven aan die pc's om bepaalde data te verzamelen. Op het moment dat de gebruiker naar zijn bankwebsite gaat, gaat hij een signaal geven naar de cybercrimineel in het botnet, dat de gebruiker naar de bankwebsite aan het gaan is. Terwijl de gebruiker dan naar de bankwebsite gaat, komt de crimineel over uw verbinding mee om zo transacties te doen. In België zijn we op dat punt nog vrij goed beveiligd, gezien de cybercrimineel de medewerking van de gebruiker nodig heeft om een transactie te kunnen doen. Dan probeert men via allerhande trucs om de gebruiker zover te krijgen om de transactie effectief te bevestigen. Het paswoord en de gebruikersnaam heeft de cybercrimineel op dat moment reeds. Het enige dat hij nog nodig heeft is dat de gebruiker met zijn digipass de transactie bevestigt. Ofwel wordt je dan gebeld, ofwel worden bijkomende schermen gepubliceerd in uw connectie met de bank onder het mom van een securitytest. Alle dossiers die te maken hebben met deze problematiek worden door het FCCU behandeld. Recentelijk krijgen we ook vaker gevallen van ransomware, waarbij mensen hun pc geblokkeerd wordt en waarbij gezegd wordt dat ze een bepaald bedrag moeten betalen om de blokkering op te heffen. Een doorsnee hacking van een facebook profiel wordt niet op het niveau van de FCCU behandeld, tenzij dit te maken heeft met een persoon die een sleutelpositie vervult binnen zo'n kritische infrastructuur. Als het bijvoorbeeld een systeembeheerder betreft, waarbij men informatie kan halen om toegang te krijgen tot die kritische infrastructuur, dan komen we wel in actie en beschouwen we dit als een deel van de hacking van de kritische infrastructuur zelf.

"Hebt u zicht op de mate waarin deze zaken ook effectief worden gevolgd door een vervolging?"

Bij die e-banking transacties liepen veel sporen naar het buitenland, daar hebben we inderdaad veel mensen kunnen identificeren, en zowel witwassers als hackers kunnen laten oppakken. Maar hier heb je dan ook weer direct dat internationaal aspect dat de kop opsteekt. Rusland gaat hun onderdanen niet uitleveren om ze hier te veroordelen en ze hier in de gevangenis te stoppen. Ze gaan die criminelen daar zelf berechten, in zoverre dat dit dan ook effectief gebeurt. We hebben in dit kader zeker al successen geboekt, al is dit niet zo duidelijk en zichtbaar als resultaat voor de Belgische justitie. Als wij immers uiteindelijk ons dossier overdragen aan die buitenlandse politiediensten, hopen wij dat zij verder het dossier afwerken en effectief iemand gaan aanhouden. Maar dat is spijtig genoeg niet telkens het geval. We hebben in bepaalde gevallen al de indruk gehad dat de vooruitgang eerder tegengehouden

werd. Ook in België hebben we al mensen geïdentificeerd en aangehouden maar het blijft wel, naar mijn gevoel, een domein dat beschouwd wordt als zijnde niet echt schadelijk voor de maatschappij. Nochtans zien we dat er meer en meer aanvallen zijn op bedrijven en organisaties.

"U bent sinds 2001 hoofd van de FCCU. Heeft u gedurende die elf jaar een evolutie vastgesteld in de manier waarop cybercrime zich manifesteert? Zijn de fenomenen talrijker geworden, en meer agressief?"

Het gegeven is veel complexer geworden, en ook agressiever. Het is zo dat hacking vroeger vaak intern geschiedde. Het betrof dan vaak medewerkers van een bedrijf die omwille van de zwakheden in het systeem, wisten hoe ze dat systeem konden misbruiken. Wat we nu zien is dat die hackingen meer van externe aard zijn, en het aantal ervan in snel tempo stijgt. Zo'n activiteit heb ik nog nooit ervaren. Wat we niet doen zijn defacements van websites, tenzij dit over kritieke infrastructuur gaat. Maar als je kijkt naar het aantal websites dat gedefaced is, op de website hashzone, dan is dat een enorm aantal, duizenden op jaarbasis. We hebben er ons een tijdje mee bezig gehouden om de overheidsdiensten en belangrijke organisaties op de hoogte te brengen dat ze gehacked waren. Het spijtige is dat men daar schijnbaar weinig belang aan hecht. We hebben voorbeelden gehad van steden waar we contact mee opnemen met de melding dat hun website is gehacked. In eerste instantie zijn die mensen verrast, maar ze ondernemen geen stappen voor een betere beveiliging, waardoor ze nog geen week later opnieuw gehacked zijn. Dat is uiterst frustrerend voor ons. Nadien hebben we dan ook beslist om dit links te laten liggen, en onze aandacht te vestigen op aanvallen op kritieke infrastructuren en te trachten de netwerken van de criminelen te destabiliseren. Dat laatste doen we vooral door servers aan te pakken die criminelen gebruiken. Dat is echter een taak die we niet alleen kunnen doen. Enerzijds, zit je weer met het internationaal aspect en, anderzijds, is er ook samenwerking nodig met de service providers. Idealiter zou iedereen meer een stuk verantwoordelijkheid moeten gaan opnemen. Op zich moeten we zeker evenveel belang hechten aan het creëren van een bewustzijn omtrent cybercriminaliteit, dan aan de bestrijding zelf. Als de eindgebruiker zich beter wapent dan zal de crimineel zijn spionagemogelijkheden verliezen, evenals zijn aanvalscapaciteit. Het is dan ook noodzakelijk dat de politie en de industrie zelf gaan samenwerken, en dat er in dit opzicht dan ook initiatieven worden genomen op wettelijk vlak, waarbij ook een verantwoordelijkheid wordt gelegd bij de eindgebruikers. Men heeft in het verleden met de wet van 13 juni 2005 betreffende de elektronische communicatie een ietwat fout signaal gegeven. In die zin dat

men de eindgebruiker als een zwakke schakel beschouwde, waar grote broer politie voor moest zorgen. Naar mijn mening is dat contraproductief. Als je met je wagen op de openbare weg rijdt moet je een rijbewijs halen en moet je auto door de keuring geraken. Als je op het internet gaat daarentegen, moet je je van niets iets aantrekken. Mensen die zonder anti-virus werken, die zeer nonchalant zijn in hun keuze van wachtwoorden, geen firewall hebben of toch blijven verder werken ook al weten ze dat ze geïnfecteerd zijn, zoeken naar mijn mening problemen.

"Beschikt de FCCU over voldoende personeel en moderne middelen om cybercrime aan te pakken?"

Momenteel zijn er bij de FCCU 35 mensen aan het werk, waarvan 10 administratief personeel. Bij de 25 Regional Computer Crime Units (RCCU's) werken zo'n 170 mensen, waarvan een 20-tal administratief personeel. Dit is niet echt voldoende, als je kijkt naar wat er verwacht wordt. Vooreerst is er het forensisch computeronderzoek in het kader van traditionele criminaliteit, zoals sociale fraude, drugs, en tegelijkertijd ook het behandelen van cybercriminaliteit. In dat opzicht is het aantal personeelsleden dan ook niet genoeg om te doen wat we moeten doen. Maar dat we met te weinig personeel kampen is een oud zeer. Op zich kan je dit enigszins beperken door in infrastructuur te investeren, waardoor je meer kan doen met minder mensen. Maar dan moeten die investeringen natuurlijk ook gebeuren, anders kom je met een structureel probleem te zitten, wat op dit moment het geval is. Reeds in 2006 werd er door de regering vooropgesteld dat er in 2011, 293 persoonsleden moesten zijn. Dat aantal is nooit bereikt, maar het markante aan de zaak is dat die berekening gebaseerd is op de behoeften die er destijds in 2006 waren. Ondertussen is de wereld compleet veranderd, en zijn die cijfers uit 2006 ook niet meer relevant. Vandaag loopt praktisch iedereen rond met een smartphone, tablets e.d.. Op de duur zit je met zoveel toestellen per gebruiker waarop inbreuken kunnen gebeuren, dat de wachtlijsten echt ellenlang worden. Ook wat budget betreft zijn we niet ruim bemeten. Het is altijd zoeken naar een werkbare oplossing, en wij passen ons aan, en doen onze best met wat we krijgen. Niettemin is wat we krijgen een minimum minimorum, als je vergelijkt welke budgetten er zijn in bijvoorbeeld Nederland, Noorwegen of Zweden. In vergelijking met die landen werken wij op minimalistische scenario's. Dit dient echter ook genuanceerd te worden; als je vergelijkt met een groot aantal andere landen, dan staan we er ook weer niet zo slecht voor.

"Kan de FCCU zich meten met Computer Crime Units uit het buitenland?"

Qua kennis en kunde die wij in huis hebben wil ik mij meten met gelijk welk ander land. Qua wettelijk kader en middelen is het natuurlijk een ander verhaal. Wat dat laatste betreft zijn we voor op de ene dienst, en ver achter op de andere. Als je kijkt naar wat er in Nederland geïnvesteerd wordt in vorming, dan kunnen wij niet anders dan jaloers zijn. De eerste die in contact komen met dergelijke misdrijven is vaak de lokale politie, die dan ook een zekere vorming dient te krijgen. In Nederland investeren ze fenomenale bedragen in de vorming van de lokale recherche, d.m.v. online cursussen e.d., uitbesteed aan private firma's. Bij ons geschiedt dat allemaal in eigen huis, wat niet houdbaar is. Nederland is dan ook koploper, niet alleen wat betreft vorming, maar ook qua opzetten van infrastructuur. Daarenboven is men daar ook creatief bezig met de bestrijding van cybercriminaliteit. Dit vooral wat betreft het afbreken van structuren die cybercriminelen gebruiken, of op z'n minst voorkomen dat het überhaupt wordt opgebouwd. De Nederlanders hebben daar dan ook een onderzoek naar opgezet, net als Luxemburg en het Verenigd Koninkrijk. België is in dat kader eerder de slechte leerling van de klas. Er is hier dan ook geen overlegstructuur of leidende overheid die de zaken gaat coördineren. Als je dan proactief moet werken moet dit gecontroleerd gebeuren, maar er is geen overheid die daar wat sturing aan geeft. Dat hebben we dan ook broodnodig. Wat de bestrijding van cybercrime betreft denk ik dat Nederland erg goed bezig is, al dienen we daar ook kanttekeningen bij te plaatsen. Men heeft daar een solide strategie opgebouwd. Men heeft trouwens in het forensisch laboratorium in Nederland een team voor digitale expertise, waar men de moeilijk gevallen van data recuperatie e.d. gaat uitvoeren. Dat is iets dat wij in België niet hebben. Hier hebben we het CERT, voor de melding van problemen waarvoor de gebruiker niet direct naar de politie wil stappen. In Nederland is een soortgelijke instelling geïntegreerd in het Nationale Cybersecurity Centre, en die instelling was 90 man groot, een enorm aantal. Ter vergelijking, het CERT is 7 man sterk. In Nederland heeft men duidelijk de keuze gemaakt om van cybercrime een prioriteit te maken, i.t.t België, waar we alles gaan willen doen, en de capaciteit dan ook als dusdanig wordt gespreid. Het probleem daarvan is dat wanneer je alles wil aanpakken, je weinig echt grondig kan doen. Je verliest als het ware capaciteit om de echt belangrijke zaken aan te pakken. In Nederland snijden ze in het aantal dossiers, maar degene die ze dan afwerken zijn ook tot op het bot uitgespit. Wat er verder ook dient te gebeuren is dat er op federaal niveau, binnen de regering, iemand moet komen die de leiding neemt inzake cyberbeveiliging. In de Verenigde Staten hebben ze dit al. Daar is Howard Schmidt de Cyber-Security Coördinator, die deel uitmaakt van het kabinet van de president zelf. Als je bijvoorbeeld kijkt naar Engeland, daar hebben ze tijdens de crisis

op zowat alles bespaard, behalve op de strijd tegen cybercriminaliteit. Integendeel, men heeft destijds ongeveer 600 miljoen pond vrijgemaakt voor de bestrijding van cybercrime. Men heeft destijds zelfs oorlogsfregatten verkocht, en de opbrengst ervan in de aanpak van cybercrime gepompt. Als je naar die investeringen kijkt, dan kan je besluiten dat we hier niet echt goed bezig zijn. Dit is echter het gevolg van het feit dat de overheid hier zich te weinig bewust lijkt te zijn van de dreiging, en de schade die cybercrime teweegbrengt. Als je dan weer vergelijkt met een land als Ierland, dan zijn we nog niet zo slecht bezig. Daar hebben ze 12 mensen die zich met cybercrime bezighouden. Wij doen het al bij al niet zo slecht, ook omwille van het feit dat wij één politiedienst hebben. Bij andere landen is dit verspreid over verschillende politiediensten, wat het werk er ook niet makkelijker op maakt. Bij de politiehervorming was het mijn taak om het FCCU op een structurele manier uit te bouwen. Dit zowel wat betreft de rekrutering van het personeel, als de opleiding, maar ook wat betreft materiaal. Dat laatste was de jaren volgend op de politiehervorming de hoofdbrok van mijn inspanningen. In die zin dat ik elk lid wou uitrusten met een forensische toren, een portable en voldoende back-up stations.

"Ik dank u voor dit interview."