RAAD VAN DE EUROPESE UNIE

Brussel, 30 mei 2011 (06.06)
(OR. en)

10751/11

Interinstitutioneel dossier: 2010/0273 (COD)

DROIPEN 47
TELECOM 82
CODEC 915

NOTA

van:	het voorzitterschap
aan:	het Coreper/de Raad
nr. vorig doc.:	10357/11 DROIPEN 42 TELECOM 74 CODEC 851
Betreft:	Voorstel voor een richtlijn van het Europees Parlement en de Raad over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad - Algemene oriëntatie

I. ACHTERGRONDINFORMATIE

Op 30 september 2010 heeft de Commissie bij het Europees Parlement en de Raad een voorstel ingediend voor een richtlijn van het Europees Parlement en de Raad over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ van de Raad.

Overeenkomstig artikel 3, lid 1, van Protocol nr. 21 bij de Verdragen hebben zowel het Verenigd Koninkrijk als Ierland de Raad ervan in kennis gesteld dat zij wensen deel te nemen aan de aanneming en de toepassing van deze richtlijn. Denemarken neemt overeenkomstig Protocol nr. 22 bij de Verdragen niet deel aan de aanneming van dit rechtsbesluit.

UK en FR maken een voorbehoud voor behandeling door het parlement. DE, SI, FR en SE maken een algemeen studievoorbehoud bij het voorstel.

Het voorstel is op 8-9 november 2010 aan de Raad voorgelegd.

Het CATS is driemaal verzocht strategische aansturing te verstrekken voor de besprekingen in de Groep materieel strafrecht (hierna Droipen). Op 13 december 2010, bij het begin van de onderhandelingen, heeft het CATS algemene richtsnoeren voor de verdere besprekingen verstrekt. Het CATS heeft op 11 februari 2011 van gedachten gewisseld over artikel 10, lid 3, van het Commissievoorstel, dat een nieuwe verzwarende omstandigheid invoert, namelijk het feit dat de cyberaanvallen gepleegd zijn met misbruik van de identiteitsgegevens van de rechtmatige eigenaar. Ten slotte is het CATS op 22 maart geraadpleegd over vier onopgeloste problemen: de reikwijdte van de bepalingen met uitzondering van onbeduidende gevallen, de bestanddelen van het in artikel 3 bedoelde strafbare feit, de strafmaat en de rechtsmacht op basis van nationaliteit.

Droipen heeft het voorstel op 13-14 en 28 januari, en op 2-3 en 29 maart 2011 besproken. Op 29 maart 2011 heeft Droipen een derde lezing van de tekst afgerond.

De Raad heeft op 25 februari 2011 nota genomen van de stand van de besprekingen. De Raad heeft op 12 april 2011 nota genomen van het voorlopig akkoord over de artikelen 1 tot en met 6, en de artikelen 11 tot en met 19 van de ontwerp-richtlijn. De Raad heeft tevens aansturing gegeven met betrekking tot verscheidene onopgeloste kwesties en aldus het politieke kader vastgesteld waarbinnen de werkzaamheden inzake het voorstel in de voorbereidende instanties van de Raad zijn voortgezet.

II. VOORSTEL VOOR EEN COMPROMISPAKKET

De tekst in bijlage dezes is een compromisvoorstel, zoals dat is voortgekomen uit de vergaderingen van de JBZ-raden van 13 mei 2011 en van de vrienden van het voorzitterschap van 24 mei 2011.

Tijdens de besprekingen is in het oorspronkelijke Commissievoorstel een aantal aanpassingen aangebracht teneinde zoveel mogelijk tegemoet te komen aan de standpunten van de delegaties. Het voorzitterschap heeft tevens getracht voldoende rekening te houden met de onderliggende reden van het Commissievoorstel, namelijk op EU-niveau voorzien in een efficiënter strafrechtelijk antwoord op de nieuwe bedreigingen van cybercriminaliteit, zoals grootschalige cyberaanvallen.

A. In dit verband wenst het voorzitterschap de voornaamste elementen van het compromispakket, die door de Raad op 12 april 2011 voorlopig zijn goedgekeurd, in herinnering te brengen.

1. Reikwijdte van de strafbaarstelling (artikelen 3 tot en met 7)

- De verwijzing naar "onbeduidende gevallen" werd uitgebreid tot alle in de richtlijn genoemde strafbare feiten (artikel 3 tot en met artikel 7). Derhalve worden onbeduidende gevallen volledig uit de werkingssfeer van de richtlijn uitgesloten. De definitie van "onbeduidende gevallen" wordt bepaald door het nationaal recht en de nationale praktijk (zie overweging 6 bis), en er worden in dat verband ook voorbeelden opgenomen.
- De werkingssfeer van artikel 3 "Onrechtmatige toegang tot informatiesystemen" werd beperkt tot de gevallen waarin de niet-naleving van een beveiligingsmaatregel een wezenlijk bestanddeel van het strafbaar feit is. In de facultatieve mogelijkheid daartoe is voorzien door het Verdrag van Boedapest, maar deze was niet in het oorspronkelijke Commissievoorstel opgenomen.
- Het bezit van instrumenten voor het plegen van cyberaanvallen werd uit de werkingssfeer van artikel 7 geweerd.
- De strafbaarstelling van pogingen tot het plegen van strafbare feiten wordt beperkt tot de in de artikelen 4 en 5 genoemde strafbare feiten.

2. Sancties (artikel 9)

- Het voorstel van de Commissie met betrekking tot de strafmaat voor de basisdelicten (zie artikel 9, lid 2), namelijk een maximale gevangenisstraf van ten minste twee jaar, blijft behouden. Dat wordt met name gerechtvaardigd door de beperkte reikwijdte van de strafbaarstelling die uit de bespreking in de voorbereidende instanties van de Raad naar voren is gekomen. De werkingssfeer van de bepaling is nog verder ingeperkt tot de artikelen 3 tot en met 6, waardoor de verplichting om in deze specifieke strafmaat te voorzien, komt te vervallen voor artikel 7.
- Het compromisvoorstel biedt meer soepelheid wat betreft de sancties bij verzwarende omstandigheden: een maximum vrijheidsstraf van ten minste drie en vijf jaar (respectievelijk lid 3 en lid 4 van artikel 9) teneinde rekening te houden met de ernst van de strafbare feiten, terwijl bovendien de toepassing van de bepalingen bij wijze van compromis wordt beperkt tot de artikelen 4 en 5.

3. Rechtsmacht (artikel 13)

- De vaststelling van de rechtsmacht ten aanzien van onderdanen wordt gekoppeld aan een positieve toetsing van de dubbele strafbaarheid (artikel 13, lid 1, onder b)).
- De voorwaarden voor de uitoefening van de nationale rechtsmacht vallen niet onder de bepalingen van de richtlijn (zie preambule, overweging 10 bis).

4. Informatie-uitwisseling over strafbare feiten in de ontwerp-richtlijn (artikel 14)

- De uiterste termijn van 8 uur voor het beantwoorden van dringende verzoeken blijft behouden, terwijl de tekst gewijzigd is om de aard van de verplichting van de aangezochte staat te verduidelijken, namelijk dat de bevoegde autoriteit binnen de vastgestelde termijn ten minste aangeeft of zij in staat zal zijn feedback te geven, en zo ja, of zij nadere toelichting kan verstrekken omtrent de voorlopige modaliteiten van de verwachte reactie, zoals de vorm of de tijdspanne waarbinnen zal worden gereageerd.

B. De werkzaamheden met betrekking tot het voorstel zijn voortgezet in het licht van de politieke aansturing die de Raad op 12 april 2011 heeft gegeven. Derhalve dienen ook de volgende nieuwe elementen in het algemene compromispakket in aanmerking te worden genomen:

1. Instrumenten voor het plegen van strafbare feiten - artikel 7

- De werkingssfeer van artikel 7 is verder beperkt. Derhalve is de productie of de beschikbaarstelling van instrumenten die kunnen worden gebruikt om cyberaanvallen uit te voeren, eveneens van de werkingssfeer van het voorstel uitgesloten.
- In de richtlijn wordt het in artikel 7 bedoelde begrip "instrument" eng opgevat, in tegenstelling tot het Commissievoorstel, dat gebaseerd was op een ruimere uitlegging van dit begrip en bijvoorbeeld speciale hardware als instrument voor het plegen van cyberaanvallen omvatte.

2. Verzwarende omstandigheden in verband met grootschalige cyberaanvallen - artikel 9

- Het kernelement van het Commissievoorstel, namelijk dat grootschalige cyberaanvallen als verzwarende omstandigheid worden beschouwd, is gehandhaafd, maar ingrijpend gewijzigd. Er moet worden benadrukt dat grootschalige cyberaanvallen twee alternatieve kenmerkende aspecten bezitten: het zijn ofwel aanvallen die gericht zijn op een groot aantal informatiesystemen ofwel aanvallen die ernstige schade veroorzaken. Deze twee aspecten worden behandeld in respectievelijk artikel 9, lid 3, en artikel 9, lid 4, onder b).

- Teneinde tegemoet te komen aan de bezwaren van verscheidene delegaties wat betreft de noodzaak om een duidelijk verband vast te stellen met de huidige dreigingen die uitgaan van bepaalde methoden die criminelen gebruiken om grootschalige cyberaanvallen uit te voeren, zoals het creëren en gebruiken van "botnets"[1], is desbetreffende tekst ingevoegd in de overwegingen bij het voorstel (zie overweging 3 en overweging 7). Het voorzitterschap heeft voor deze aanpak gekozen teneinde in het dispositief van de richtlijn de nodige soepelheid en technische neutraliteit te handhaven wat betreft de methoden om grootschalige cyberaanvallen uit te voeren. Dit is bijzonder relevant gezien de onophoudelijke technologische vooruitgang en de voortdurend evoluerende aard van deze vorm van criminaliteit.

- Bij wijze van compromis is artikel 9, lid 5, betreffende het misbruik van de persoonsgegevens van een andere persoon dan de dader met het oogmerk het vertrouwen van een derde partij te winnen teneinde cyberaanvallen te vergemakkelijken, geschrapt. Dit was het gevolg van het constant door bepaalde delegaties tot uitdrukking gebrachte standpunt dat het hier een verschijnsel betreft dat op een alomvattende manier moet worden aangepakt in een specifiek aan de strijd tegen identiteitsdiefstal gewijd instrument.

---

[1] Kenmerkend voor zogenaamde "botnets" is dat de strafbare handeling in opeenvolgende fasen plaatsvindt, waarbij iedere fase afzonderlijk ernstig gevaar voor openbare belangen kan opleveren. In dit verband is de richtlijn er onder meer op gericht strafrechtelijke sancties in te voeren voor de fase waar de "botnet" wordt gecreëerd, namelijk wanneer controle op afstand over een aanzienlijk aantal computers tot stand wordt gebracht door deze door middel van gerichte cyberaanvallen te besmetten met kwaadaardige software. In een latere fase kunnen de besmette computers, die de "botnet" vormen, zonder medeweten van hun gebruikers worden ingezet om een grootschalige cyberaanval uit te voeren, die gewoonlijk het vermogen heeft om ernstige schade te veroorzaken.

3. Rechtsmacht (overweging 10 bis)

- In de herziene formulering van overweging 10 bis wordt een duidelijk onderscheid gemaakt tussen de voorwaarden voor het vestigen van rechtsmacht, als bedoeld in artikel 13, en de voorwaarden voor de uitoefening van rechtsmacht.

Het Coreper wordt verzocht
a) de nieuwe elementen van het compromis in aanmerking te nemen als integraal deel van het algemene voorstel voor een compromispakket en
b) te bevestigen dat de tekst, vervat in de bijlage, aan de Raad moet worden voorgelegd teneinde een algemene oriëntatie over het voorstel vast te stellen, zodat de bijgaande tekst als basis kan dienen voor de verdere besprekingen met het Europees Parlement, overeenkomstig artikel 294 van het VWEU.

2010/0273 (COD)

Voorstel voor een

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD

over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,
Gezien het Verdrag betreffende de werking van de Europese Unie, en met name
artikel 83, lid 1,
Gezien het voorstel van de Europese Commissie,[2]
Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,
Gezien het advies van het Europees Economisch en Sociaal Comité,
Gezien het advies van het Comité van de Regio's,
Handelend volgens de gewone wetgevingsprocedure,
Overwegende hetgeen volgt:

(1) Deze richtlijn heeft ten doel de strafwetgeving van de lidstaten inzake aanvallen op informatiesystemen onderling af te stemmen door minimumvoorschriften vast te stellen voor de definitie van strafbare feiten en sancties op dit gebied, en de samenwerking tussen de bevoegde autoriteiten, zoals de politie en andere gespecialiseerde rechtshandhavings-instanties van de lidstaten, te verbeteren.

(2) Aanvallen op informatiesystemen, in het bijzonder in het kader van de georganiseerde criminaliteit, vormen een groeiende bedreiging en de bezorgdheid over mogelijke terroristische of politiek gemotiveerde aanvallen op informatiesystemen die deel uitmaken van de kritieke infrastructuur van de lidstaten en de Unie neemt toe. Dit brengt de totstandbrenging van een veiliger informatiemaatschappij en een ruimte van vrijheid, veiligheid en recht in gevaar en maakt derhalve een reactie op het niveau van de Europese Unie noodzakelijk.

[2] PB C […] van […], blz. […].

(2 bis) Ontwrichting of vernietiging van bepaalde kritieke infrastructuren in de Unie zou aanzienlijke grensoverschrijdende gevolgen hebben. Uit de behoefte aan een grotere capaciteit tot bescherming van de kritieke infrastructuur in Europa blijkt dat in het kader van de bestrijding van aanvallen op informatiesystemen moet worden voorzien in zware strafrechtelijke sancties die in verhouding staan tot de ernst van deze aanvallen. Onder "kritieke infrastructuur" kan worden verstaan een voorziening, systeem of een deel daarvan op het grondgebied van een lidstaat dat van essentieel belang is voor bijvoorbeeld het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn van de bevolking, en waarvan de ontwrichting of vernietiging in een lidstaat aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken.

(3) Er zijn aanwijzingen dat grootschalige aanvallen op de informatiesystemen die vaak van vitaal belang kunnen zijn voor staten of voor specifieke onderdelen van de publieke of particuliere sector steeds gevaarlijker en frequenter worden. Deze tendens gaat gepaard met de ontwikkeling van steeds geavanceerder (…) methoden, zoals het creëren en gebruiken van zogenaamde "botnets". Kenmerkend hierbij is dat de strafbare handeling in opeenvolgende fasen plaatsvindt, waarbij iedere fase afzonderlijk ernstig gevaar voor openbare belangen kan opleveren. In dit verband is de richtlijn er onder meer op gericht strafrechtelijke sancties in te voeren voor de fase waar de "botnet" wordt gecreëerd, namelijk wanneer controle op afstand over een aanzienlijk aantal computers tot stand wordt gebracht door deze door middel van gerichte cyberaanvallen te besmetten met kwaadaardige software. In een latere fase kunnen de besmette computers, die de "botnet" vormen, zonder medeweten van hun gebruikers worden ingezet om een grootschalige cyberaanval uit te voeren, die gewoonlijk het vermogen heeft om ernstige schade te veroorzaken, als bedoeld in deze richtlijn. De lidstaten kunnen bepalen wat overeenkomstig hun nationaal recht en hun nationale praktijk onder ernstige schade wordt verstaan; het kan daarbij onder meer gaan om ontregelde systeemdiensten van groot openbaar belang, aanzienlijke financiële kosten of verlies van persoonsgegevens.

(4) Gemeenschappelijke definities op dit gebied, en in het bijzonder van informatiesystemen en computergegevens, zijn van belang om te garanderen dat de richtlijn in de lidstaten coherent wordt toegepast.

(5) Teneinde tot een gemeenschappelijke aanpak van de bestanddelen van strafbare feiten te komen, moet een gemeenschappelijke definitie worden ingevoerd van onrechtmatige toegang tot een informatiesysteem, onrechtmatige systeemverstoring, onrechtmatige gegevensverstoring en onrechtmatige onderschepping.

(6) De lidstaten dienen aanvallen op informatiesystemen strafbaar te stellen. De straffen dienen doeltreffend, evenredig en afschrikkend te zijn.

(6 bis) De richtlijn voorziet in elk geval in strafrechtelijke sancties voor gevallen die niet onbeduidend zijn. De lidstaten kunnen volgens hun nationaal recht en hun nationale praktijk bepalen welke gevallen onbeduidende gevallen zijn. Het geval kan bijvoorbeeld als onbeduidend worden beschouwd wanneer de schade en/of het gevaar dat het oplevert voor openbare of particuliere belangen, zoals de integriteit van een computersysteem of van computergegevens, of de integriteit, de rechten en andere belangen van een persoon, onbeduidend zijn of van dien aard zijn dat het opleggen van een strafrechtelijke sanctie binnen de door de wet bepaalde minima en maxima of het strafrechtelijk aansprakelijk stellen voor deze feiten niet noodzakelijk is.

(7) Het is passend om te voorzien in zwaardere straffen voor aanvallen op een informatiesysteem die gepleegd worden door een criminele organisatie in de zin van Kaderbesluit 2008/841/JBZ van de Raad van 24 oktober 2008 ter bestrijding van georganiseerde criminaliteit[3] of voor grootschalige aanvallen, die een groot aantal informatiesystemen treffen of ernstige schade veroorzaken, met inbegrip van aanvallen die tot doel hadden een "botnet" te creëren of die werden uitgevoerd door middel van een "botnet", en aldus ernstige schade veroorzaken (…).

(8) De conclusies van de Raad van 27 en 28 november 2008 hielden in dat er binnen de lidstaten en de Commissie een nieuwe strategie dient te worden ontwikkeld, waarbij rekening wordt gehouden met de inhoud van het uit 2001 daterende Verdrag inzake cybercriminaliteit van de Raad van Europa. Dat verdrag is het wettelijke referentiekader voor de bestrijding van cybercriminaliteit, waaronder aanvallen op informatiesystemen. Deze richtlijn bouwt daarop voort.

(9) Gelet op de verschillende manieren waarop aanvallen kunnen worden uitgevoerd, en gelet op de snelle ontwikkelingen op het gebied van hardware en software, wordt er in deze richtlijn verwezen naar "instrumenten" die kunnen worden gebruikt voor het plegen van de in deze richtlijn opgesomde strafbare feiten. Onder instrumenten wordt bijvoorbeeld kwaadaardige software verstaan, zoals die voor het creëren van botnets, waarmee cyberaanvallen worden gepleegd. Aangezien in deze richtlijn minimumvoorschriften worden vastgesteld, kunnen de lidstaten in strafrechtelijke sancties voorzien voor andere soorten delicten, met betrekking tot de instrumenten die zijn gebruikt om de delicten te plegen, zoals het bezit van die instrumenten of de productie, de verkoop, de aanschaf voor gebruik, de invoer, de verspreiding of het op andere wijze beschikbaar maken van andere instrumenten, met inbegrip van hardware, die hoofdzakelijk zijn ontworpen of aangepast om de in de richtlijn bedoelde delicten te plegen.

---

[3] PB L 300 van 11.11.2008, blz. 42.

(10) Deze richtlijn beoogt niet de strafbaarstelling van feiten die gepleegd worden zonder criminele opzet, zoals het officieel testen of beveiligen van informatiesystemen, of zonder dat de betrokkene zich ervan bewust was dat de toegang niet was toegestaan.

(10 bis) Deze richtlijn betreft niet de voorwaarden waaraan voldaan dient te worden voor (…) de uitoefening van rechtsmacht met betrekking tot een van de in de artikelen 3 tot en met 8 genoemde strafbare feiten, zoals een aangifte die door het slachtoffer is gedaan op de plaats waar de feiten zijn gepleegd, een aanklacht die is geformuleerd door de staat van de plaats waar de feiten zijn gepleegd of het feit dat de dader niet vervolgd is op de plaats waar de feiten zijn gepleegd.

(11) Deze richtlijn vergroot het belang van netwerken, zoals dat van de G8 of het netwerk van meldpunten van de Raad van Europa, die vierentwintig uur per dag en zeven dagen per week voor informatie-uitwisseling bereikbaar zijn om te waarborgen dat de beschikbare relevante gegevens kunnen worden verstrekt voor onderzoeken of procedures inzake strafbare feiten op het gebied van informatiesystemen en gegevens die de verzoekende lidstaat aanbelangen. Gelet op de snelheid waarmee grootschalige aanvallen kunnen worden uitgevoerd, dienen alle lidstaten onverwijld te kunnen reageren op dringende bijstandsverzoeken van dit netwerk van meldpunten. In deze gevallen moet in het verzoek tot het verstrekken van gegevens een telefonisch te bereiken contactpersoon worden vermeld, teneinde te waarborgen dat het verzoek spoedig door de aangezochte staat kan worden behandeld en dat binnen 8 uur feedback wordt gegeven, met melding van de ontvangst van het verzoek, alsook van een indicatie of en, zo ja, wanneer het naar alle waarschijnlijkheid zal worden ingewilligd.

(12) Er dienen gegevens te worden verzameld over strafbare feiten in de zin van deze richtlijn, zodat er een volledi ger beeld ontstaat van het probleem op het niveau van de Unie en er doeltreffender antwoorden kunnen worden geformuleerd. Met behulp van deze gegevens kunnen gespecialiseerde agentschappen zoals Europol en het Europees Agentschap voor netwerk- en informatiebeveiliging de omvang van cybercriminaliteit en de netwerk- en informatiebeveiliging in Europa bovendien beter beoordelen.

(13) Grote lacunes en verschillen in de wetgeving van de lidstaten op het gebied van aanvallen op informatiesystemen kunnen een belemmering vormen voor de bestrijding van georganiseerde criminaliteit en terrorisme, en kunnen doeltreffende politiële en justitiële samenwerking op dit gebied bemoeilijken. Het transnationale grensloze karakter van moderne informatiesystemen houdt in dat aanvallen op deze systemen een grensoverschrijdende dimensie hebben, wat tot gevolg heeft dat er dringend behoefte bestaat aan verdere onderlinge afstemming van het strafrecht op dit gebied. Bovendien dient de coördinatie van de vervolging van aanvallen op informatiesystemen te worden vergemakkelijkt door de vaststelling van Kaderbesluit 2009/948/JBZ van de Raad over het voorkomen en beslechten van geschillen over de uitoefening van rechtsmacht bij strafprocedures.

(14) Aangezien de doelstellingen van deze richtlijn om aanvallen op informatiesystemen in alle lidstaten te bestraffen met doeltreffende, evenredige en afschrikkende straffen en om de justitiële samenwerking te verbeteren en te bevorderen door mogelijke moeilijkheden weg te nemen, niet in voldoende mate door de lidstaten kunnen worden verwezenlijkt, omdat de regels gemeenschappelijk en met elkaar verenigbaar moeten zijn, en deze doelstellingen dus beter op het niveau van de Europese Unie kunnen worden verwezenlijkt, kan de Unie maatregelen nemen, in overeenstemming met het in artikel 5 van het Verdrag betreffende de Europese Unie omschreven subsidiariteitsbeginsel. Deze richtlijn gaat niet verder dan wat nodig is om voornoemde doelstellingen te verwezenlijken.

(15) De persoonsgegevens die worden verwerkt in het kader van de uitvoering van deze richtlijn dienen te worden beschermd overeenkomstig de regels van Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 inzake de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken[4] (met betrekking tot de verwerkingswerkzaamheden die binnen het toepassingsgebied daarvan vallen) en Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens.[5]

---

[4] PB L 350 van 30.12.2008, blz. 60.

[5] PB L 8 van 12.1.2001, blz. 1.

(16) Deze richtlijn eerbiedigt de grondrechten en is in overeenstemming met de beginselen die met name bij het Handvest van de grondrechten van de Europese Unie zijn erkend, waaronder de bescherming van persoonsgegevens, de vrijheid van meningsuiting en van informatie, het recht op een eerlijk proces en het beginsel van het vermoeden van onschuld, alsmede het legaliteitsbeginsel en het evenredigheidsbeginsel inzake delicten en straffen. Deze richtlijn beoogt in het bijzonder de onverkorte eerbiediging van deze rechten en beginselen te waarborgen en moet dienovereenkomstig worden uitgevoerd.

(17) Overeenkomstig artikel (…) 3 (…) van het Protocol betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, dat gehecht is aan het Verdrag betreffende de werking van de Europese Unie, hebben het Verenigd Koninkrijk en Ierland kennis gegeven van hun wens om aan de goedkeuring en toepassing van deze richtlijn deel te nemen.

(18) Overeenkomstig de artikelen 1 en 2 van het Protocol betreffende de positie van Denemarken, dat gehecht is aan het Verdrag betreffende de werking van de Europese Unie, neemt Denemarken niet deel aan de goedkeuring van deze richtlijn en is het dus niet gebonden door, noch onderworpen aan de toepassing van deze richtlijn.

(19) Deze richtlijn strekt tot wijziging en uitbreiding van de bepalingen van Kaderbesluit 2005/222/JBZ. Aangezien de aan te brengen wijzigingen talrijk en ingrijpend zijn, dient het kaderbesluit ter wille van de duidelijkheid integraal te worden vervangen voor de lidstaten die aan de aanneming van deze richtlijn deelnemen.

(20) Overeenkomstig punt 34 van het Interinstitutioneel Akkoord "Beter wetgeven"[6] worden de lidstaten ertoe aangespoord voor zichzelf en in het belang van de Unie hun eigen tabellen op te stellen, en daarin, voor zover mogelijk, het verband weer te geven tussen deze richtlijn en de omzettingsmaatregelen, en deze tabellen openbaar te maken.

[6] PB C 321 van 31.12.2003, blz. 1.

HEBBEN DE VOLGENDE RICHTLIJN VASTGESTELD:

Artikel 1

Onderwerp

Deze richtlijn stelt minimumvoorschriften vast voor de definitie van strafbare feiten en sancties op het gebied van aanvallen op informatiesystemen. Zij strekt er tevens toe de preventie van deze strafbare feiten te vergemakkelijken en de samenwerking tussen de justitiële en de andere bevoegde autoriteiten te verbeteren.

Artikel 2

Definities

In deze richtlijn wordt verstaan onder:

a) "informatiesysteem": apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken, alsmede de computergegevens die daarmee worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud daarvan;

b) "computergegevens": elke weergave van feiten, gegevens of begrippen in een vorm die geschikt is voor verwerking in een informatiesysteem, met inbegrip van programma's die een informatiesysteem een bepaalde functie kunnen laten vervullen;

c) "rechtspersoon": ieder lichaam dat deze hoedanigheid krachtens het toepasselijke recht bezit, met uitzondering van staten of andere overheidslichamen in de uitoefening van het openbaar gezag en van publiekrechtelijke internationale organisaties;

d) "onrechtmatig": toegang, verstoring, onderschepping of enige andere in deze richtlijn genoemde gedraging die niet is toegestaan door de eigenaar of een andere houder van rechten op het systeem of op een deel daarvan, of niet is toegestaan krachtens de nationale wetgeving.

Artikel 3

Onrechtmatige toegang tot informatiesystemen

De lidstaten treffen de nodige maatregelen om onrechtmatige toegang tot een informatiesysteem of tot een deel ervan, strafbaar te stellen wanneer deze opzettelijk is geschied, en in elk geval wanneer het strafbaar feit is gepleegd door het overtreden van een beveiligingsmaatregel en voor gevallen die niet onbeduidend zijn.

Artikel 4

Onrechtmatige systeemverstoring

De lidstaten treffen de nodige maatregelen om het ernstig hinderen of het onderbreken van de werking van een informatiesysteem, door de invoer, de transmissie, het beschadigen, wissen, verminken, wijzigen, onderdrukken of ontoegankelijk maken van computergegevens, indien dat opzettelijk en op onrechtmatige wijze geschiedt, strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.

Artikel 5

Onrechtmatige gegevensverstoring

De lidstaten treffen de nodige maatregelen om het wissen, beschadigen, verminken, wijzigen, onderdrukken of ontoegankelijk maken van computergegevens in een informatiesysteem, indien dat opzettelijk en op onrechtmatige wijze geschiedt, strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.

Artikel 6

Onrechtmatige onderschepping

De lidstaten treffen de nodige maatregelen om het met technische middelen onderscheppen van niet-openbare transmissies van computergegevens naar, vanuit of binnen een computersysteem, met inbegrip van elektromagnetische emissies uit een computersysteem dat zulke computergegevens draagt, indien dat opzettelijk en op onrechtmatige wijze geschiedt, strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.

Artikel 7

Instrumenten voor het plegen van strafbare feiten

1) De lidstaten treffen de nodige maatregelen om de productie, de verkoop, de aanschaf voor gebruik, de invoer, de verspreiding of het op andere wijze beschikbaar maken van de volgende zaken, indien dat opzettelijk en op onrechtmatige wijze geschiedt, met het oogmerk deze te gebruiken voor het plegen van een van de in de artikelen 3 tot en met 6 bedoelde feiten, strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn:

a) een computerprogramma, dat hoofdzakelijk ontworpen of aangepast is voor het plegen van de in de artikelen 3 tot en met 6 bedoelde strafbare feiten;

b) een computerwachtwoord, toegangscode of soortgelijke gegevens die toegang bieden tot een informatiesysteem of een deel daarvan.

Artikel 8

Uitlokking, deelneming, medeplichtigheid en poging

1. De lidstaten zorgen ervoor dat uitlokking van, alsmede deelneming en medeplichtigheid aan een van de in de artikelen 3 tot en met 7 genoemde feiten strafbaar wordt gesteld.

2. De lidstaten zorgen ervoor dat poging tot het plegen van een van de in de artikelen 4 en 5 genoemde feiten strafbaar wordt gesteld.

Artikel 9

Sancties

1. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 3 tot en met 8 bedoelde feiten strafbaar worden gesteld met doeltreffende, evenredige en afschrikkende strafrechtelijke sancties.

2. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 3 tot en met 6 bedoelde feiten strafbaar worden gesteld met een maximale gevangenisstraf van ten minste twee jaar.

3. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 4 en 5 bedoelde feiten, wanneer deze opzettelijk worden gepleegd, strafbaar worden gesteld met een maximale gevangenisstraf van ten minste drie jaar, wanneer (…) een groot aantal informatiesystemen getroffen zijn door het (…) gebruik van een in artikel 7, lid 1, bedoeld instrument, dat hoofdzakelijk voor dit doel is ontworpen of aangepast[7].

4. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 4 en 5 bedoelde feiten strafbaar worden gesteld met een maximale gevangenisstraf van ten minste vijf jaar wanneer het strafbare feit

a) is gepleegd in het kader van een criminele organisatie zoals omschreven in Kaderbesluit 2008/814/JBZ van de Raad, ongeacht de daarin aangegeven strafmaat, of
b) ernstige schade heeft teweeggebracht[8], of
c) is gepleegd tegen een informatiesysteem dat deel uitmaakt van de kritieke infrastructuur.

(…)

[…]

Artikel 11

Aansprakelijkheid van rechtspersonen

1. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat rechtspersonen aansprakelijk kunnen worden gesteld voor de in de artikelen 3 tot en met 8 genoemde strafbare feiten wanneer die feiten tot hun voordeel zijn gepleegd door personen die hetzij individueel, hetzij als lid van een orgaan van de rechtspersoon optreden en die in de rechtspersoon een leidende functie bekleden op grond van:

a) de bevoegdheid om de rechtspersoon te vertegenwoordigen;

[7] FR, ES, en EE maken een studievoorbehoud. LV kan dit voorstel niet steunen.
[8] RO maakt een studievoorbehoud bij artikel 9, lid 4, onder b).

b) de bevoegdheid om namens de rechtspersoon beslissingen te nemen;

c) de bevoegdheid om binnen het kader van de rechtspersoon controle uit te oefenen.

2. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat rechtspersonen aansprakelijk kunnen worden gesteld indien het gebrek aan toezicht of controle door een in lid 1 bedoelde persoon het voor een persoon die onder het gezag van de rechtspersoon staat, mogelijk heeft gemaakt ten voordele van die rechtspersoon een van de in de artikelen 3 tot en met 8 bedoelde strafbare feiten te plegen.

3. De aansprakelijkheid van rechtspersonen krachtens de leden 1 en 2 sluit strafvervolging van natuurlijke personen die een in de artikelen 3 tot en met 8 bedoeld strafbaar feit plegen, uitlokken of eraan medeplichtig zijn, niet uit.

Artikel 12

Sancties tegen rechtspersonen

1. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat tegen een rechtspersoon die uit hoofde van artikel 11, lid 1, aansprakelijk is gesteld, doeltreffende, evenredige en afschrikkende sancties kunnen worden vastgesteld, waaronder strafrechtelijke of niet-strafrechtelijke geldboetes en eventueel andere sancties, zoals:
   a) uitsluiting van door de overheid verleende voordelen of steun;
   b) een tijdelijk of permanent verbod op het uitoefenen van commerciële activiteiten;
   c) plaatsing onder toezicht van de rechter;
   d) gerechtelijke ontbinding;
   e) tijdelijke of permanente sluiting van vestigingen die zijn gebruikt voor het plegen van het strafbare feit.
2. De lidstaten treffen de nodige maatregelen opdat tegen een rechtspersoon die volgens artikel 11, lid 2, aansprakelijk is, sancties kunnen worden vastgesteld of maatregelen kunnen worden getroffen die doeltreffend, evenredig en afschrikkend zijn.

Artikel 13
Rechtsmacht [9]

1. Iedere lidstaat vestigt zijn rechtsmacht ten aanzien van de in de artikelen 3 tot en met 8 genoemde strafbare feiten indien deze:

   a) geheel of gedeeltelijk op zijn grondgebied zijn gepleegd; of

   b) door een van zijn onderdanen zijn gepleegd, in elk geval voor zover het feit een strafbaar feit is op de plaats waar het is gepleegd.

2. Bij het vestigen van zijn rechtsmacht overeenkomstig lid 1, onder a), zorgt elke lidstaat ervoor dat deze zich uitstrekt tot gevallen waarin:

   a) de dader het strafbare feit pleegt terwijl hij zich fysiek op het grondgebied van die lidstaat bevindt, ongeacht of het strafbare feit is gericht tegen een informatiesysteem op dat grondgebied, of

   b) het strafbare feit gericht is tegen een informatiesysteem op het grondgebied van de betrokken lidstaat, ongeacht of de dader het strafbare feit pleegt terwijl hij zich fysiek op het grondgebied van die lidstaat bevindt.

3. Elke lidstaat stelt de Commissie in kennis van zijn besluit om zijn rechtsmacht te vestigen over een strafbaar feit in de zin van de artikelen 3 en 8 dat buiten zijn grondgebied is gepleegd, indien het strafbare feit is gepleegd:

   a) door iemand die gewoonlijk op zijn grondgebied verblijft; of

   b) ten voordele van een rechtspersoon die gevestigd is op het grondgebied van die lidstaat.

---

9 UK handhaaft een studievoorbehoud bij dit artikel.

Artikel 14

Informatie-uitwisseling[10]

1. Voor informatie-uitwisseling over strafbare feiten in de zin van de artikelen 3 tot en met 8 maken de lidstaten gebruik van het bestaande netwerk van operationele meldpunten die vierentwintig uur per dag en zeven dagen per week bereikbaar zijn. De lidstaten zorgen er tevens voor dat zij over procedures beschikken waarmee zij binnen maximaal acht uur kunnen aangeven of het verzoek om bijstand zal worden ingewilligd, alsmede de vorm en het tijdstip waarop dit naar verwachting zal gebeuren.

2. De lidstaten stellen de Commissie in kennis van het meldpunt dat is aangewezen voor de informatie-uitwisseling over in de artikelen 3 tot en met 8 bedoelde strafbare feiten. De Commissie geeft deze informatie door aan de overige lidstaten.

Artikel 15

Toetsing en statistieken[11]

1. De lidstaten zorgen voor een systeem voor het registreren, aanmaken en verstrekken van statistische gegevens over de in de artikelen 3 tot en met 7 bedoelde strafbare feiten.

2. De in lid 1 bedoelde statistieken vermelden ten minste de beschikbare gegevens over het aantal in de artikelen 3 tot en met 7 bedoelde strafbare feiten die door de lidstaten zijn geregistreerd en het aantal personen dat is vervolgd en veroordeeld in verband met de in de artikelen 3 tot en met 7 bedoelde strafbare feiten.

3. De lidstaten verstrekken de overeenkomstig dit artikel verzamelde gegevens aan de Commissie. De Commissie zorgt er tevens voor dat een geconsolideerd overzicht van hun statistische verslagen wordt gepubliceerd.

---

10 Studievoorbehoud van ES.
11 Studievoorbehoud van ES.

Artikel 16

Vervanging van Kaderbesluit 2005/222/JBZ[12]

Bij dezen wordt Kaderbesluit 2005/222/JBZ vervangen voor de lidstaten die aan de aanneming van deze richtlijn deelnemen, onverminderd de verplichtingen van de lidstaten wat betreft de termijn voor de omzetting van het kaderbesluit in nationaal recht.

Voor lidstaten die aan de aanneming van deze richtlijn deelnemen, worden verwijzingen naar Kaderbesluit 2005/222/JBZ gelezen als verwijzingen naar deze richtlijn.

Artikel 17

Omzetting

1. De lidstaten doen de nodige wettelijke en bestuursrechtelijke bepalingen in werking treden om uiterlijk op [twee jaar na aanneming] aan deze richtlijn te voldoen.

2. De lidstaten delen aan de Commissie de tekst mede van alle bepalingen waarmee zij hun verplichtingen uit hoofde van deze richtlijn in hun nationaal recht omzetten.

3. Wanneer de lidstaten deze bepalingen aannemen, wordt in de bepalingen zelf of bij de officiële bekendmaking daarvan naar deze richtlijn verwezen. De regels voor deze verwijzing worden vastgesteld door de lidstaten.

Artikel 18

Verslaglegging

1. De Commissie dient uiterlijk op [VIER JAAR NA AANNEMING] bij het Europees Parlement en de Raad een verslag in waarin wordt beoordeeld in hoeverre de lidstaten de nodige maatregelen hebben genomen om aan deze richtlijn te voldoen, indien nodig vergezeld van wetgevingsvoorstellen.

(…)

12 UK handhaaft een studievoorbehoud.

Artikel 19

Inwerkingtreding

Deze richtlijn treedt in werking op de dag van haar bekendmaking in het Publicatieblad van de Europese Unie.

Artikel 20

Adressaten

Deze richtlijn is overeenkomstig de Verdragen gericht tot de lidstaten.

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*