Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

34 034 Implementatie van de richtlijn 2013/40/EU van het Europees parlement en de Raad over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PbEU L 218/8)

Nr. 3

Het advies van de Afdeling advisering van de Raad van State wordt niet openbaar gemaakt, omdat het zonder meer instemmend luidt / uitsluitend opmerkingen van redactionele aard bevat (artikel 26, vijfde lid, van de Wet op de Raad van State).

MEMORIE VAN TOELICHTING[1]

Algemeen

1. Inleiding

Dit wetsvoorstel strekt tot implementatie van de richtlijn 2013/40/EU van het Europees parlement en de Raad van 12 augustus 2013 over aanvullen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PbEU L 218/8)(hierna: de richtlijn). De implementatietermijn van de richtlijn loopt af op 4 september 2015 (artikel 16 van de richtlijn). Vóór die datum dient de richtlijn door de lidstaten op nationaal niveau te zijn omgezet. Een transponeringstabel is in de bijlage bij deze memorie van toelichting opgenomen.

De implementatie van de richtlijn leidt tot enkele aanscherpingen van strafbaarstellingen van computercriminaliteit in het Wetboek van Strafrecht. De wijzigingen betreffen enkele verhogingen van strafmaxima en de toevoeging van een aantal strafverzwarende omstandigheden aan de computerdelicten.

De Tweede en Eerste Kamer zijn tijdens de totstandkoming van deze richtlijn geïnformeerd over de stand van zaken (zie onder meer Kamerstukken II 2010/11, 22 112, nr. 1082, Kamerstukken II 2010/11, 32 317, nrs. 27, 44, 50, 66, Kamerstukken I 2010/11, 32 317, AE, AJ, AR en S, Kamerstukken II 2011/12, 32 317, nrs. 124 en 136, Kamerstukken I 2011/12, 32 317, BW en CA, Kamerstukken I 2012/13, 32 317, CU).

De richtlijn bouwt voort op het Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18; hierna: het Cybercrimeverdrag) en vervangt het bestaande kaderbesluit uit 2005 (Kaderbesluit 2005/222/JBZ van 24 februari 2005 over aanvallen op informatiesystemen; PbEU L 69/67; hierna: het kaderbesluit). De richtlijn bevat enkele aanvullingen ten opzichte van het kaderbesluit.

[1] De oorspronkelijke tekst van het voorstel van wet en van de memorie van toelichting zoals voorgelegd aan de Afdeling advisering van de Raad van State is ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

kst-34034-3
ISSN 0921 - 7371
's-Gravenhage 2014

Voor een deel zijn deze aanvullingen ontleend aan het Cybercrimeverdrag. Voor een deel zijn deze aanvullingen, ook ten opzichte van het Cybercrimeverdrag, nieuw. Het betreft met name de bepalingen over de strafmaxima en strafverzwarende omstandigheden.
Dit kabinet onderkent de toenemende risico's van cybercriminaliteit en wil dit fenomeen krachtig aanpakken. Ik verwijs ook naar het wetsvoorstel tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van cybercrime (computercriminaliteit III), waarover de Afdeling advisering van de Raad van State advies heeft uitgebracht. De aanpak wordt door de bepalingen uit de richtlijn versterkt.

Maatschappelijke en economische processen zijn in sterke mate afhankelijk van ICT. Van cybercriminaliteit gaan dan ook grote dreigingen uit, zoals bijvoorbeeld gevaar voor maatschappelijke ontwrichting en voor het vertrouwen in het financieel-economische systeem. Dat risico is vooral aan de orde bij aanvallen via zogenoemde «botnets», waarbij controle op afstand over een aanzienlijk aantal computers tot stand wordt gebracht door deze door middel van gerichte cyberaanvallen te besmetten met kwaadaardige software. Als het eenmaal tot stand is gekomen, kan het netwerk van computers dat de «botnet» vormt, zonder medeweten van de gebruikers ervan, worden ingezet om een grootschalige cyberaanval uit te voeren, die ernstige schade kan veroorzaken. Grootschalige cyberaanvallen kunnen onder andere ernstige economische schade veroorzaken doordat informatiesystemen uitvallen en communicatie wordt onderbroken en doordat er commercieel vertrouwelijke of andere gegevens verloren gaan of worden gewijzigd. Ontwrichting en vernietiging van vitale infrastructuren, zoals energiecentrales, vervoersnetwerken en overheidsnetwerken, kunnen aanzienlijke gevolgen hebben. De strafrechtelijke aanpak van computercriminaliteit bestaat uit een samenstel van maatregelen op het gebied van het opsporen van de plegers daarvan, het ontmantelen van criminele infrastructuren, het tegenhouden van crimineel handelen en het waarschuwen van slachtoffers. Daartoe worden incident (dadergerichte) onderzoeken op basis van meldingen of aangiften uitgevoerd, naast fenomeengerichte onderzoeken op basis van meer algemene sturingsinformatie. Hierdoor worden acute dreigingen aangepakt en wordt gewerkt aan een meer generieke veiligheid op het internet.
In verband met de naar zijn aard veelal grensoverschrijdende cybercriminaliteit en grensoverschrijdende gevolgen is het noodzakelijk om een gezamenlijke Europese aanpak te ontwikkelen. Dit voorkomt «safe havens». Voorkomen moet worden dat personen (via computers) in landen waar bepaalde feiten niet strafbaar zijn gesteld of met een lage straf worden bedreigd, computercriminaliteit ten aanzien van de Nederlandse overheid, Nederlandse bedrijven en burgers kunnen plegen. Bovendien is het vanwege het grensoverschrijdend karakter veelal niet mogelijk om een verdachte (alleen) in Nederland op te sporen en te vervolgen, terwijl de gevolgen van criminaliteit wel in Nederland neerslaan en gestopt moeten worden. Relaties met zowel de herkomstlanden als landen waar veel prioriteit wordt gegeven aan de aanpak van computercriminaliteit – waar veel ervaring en expertise voorhanden is – dragen daaraan bij. Voor de internationale samenwerking zijn internationale instrumenten, zoals het Cybercrimeverdrag en de richtlijn die met dit wetsvoorstel wordt geïmplementeerd, van groot belang.

Om beter weerstand te kunnen bieden aan de problematiek is er daarnaast behoefte aan het verzamelen – op EU niveau – van vergelijkbare (statistische) gegevens over de in de richtlijn bedoelde strafbare feiten. Met behulp van deze gegevens, zoals bijvoorbeeld over modus operandi en frequentie, kunnen dreigingsevaluaties en strategische evaluaties van

cybercriminaliteit worden uitgevoerd. Op basis daarvan kan een beter inzicht ontstaan in huidige en toekomstige dreigingen en kunnen meer passende en gerichte besluiten worden genomen over het bestrijden en voorkomen van aanvallen op informatiesystemen. Het verzamelen en doorgeven van dergelijke gegevens sluiten aan bij de huidige werkzaamheden van het Team High Tech Crime (THTC) van de Dienst Nationale Recherche van de Landelijke Eenheid van de Nationale Politie, dat nu al het 24/7 contactpunt voor andere staten is als het gaat om de bestrijding van cybercrime door Nederland en bij de huidige werkzaamheden van het Nationaal Cyber Security Centrum van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Beide organisaties beschikken ook al over vaste contacten met enerzijds Europol en anderzijds de European Union Agency for Network and Information Security (ENISA).

Over dit wetsvoorstel zijn adviezen ontvangen van het openbaar ministerie (OM), de Nederlandse Vereniging voor Rechtspraak (NVvR) en de Raad voor de rechtspraak (Rvdr)[2]. De NOvA heeft aangegeven geen advies te zullen uitbrengen. De Nationale Politie heeft geen gebruikgemaakt van de geboden gelegenheid om een advies uit te brengen.

Het OM heeft aangegeven met belangstelling te hebben kennisgenomen van het wetsvoorstel. Het ziet geen aanleiding om bij het wetsvoorstel als zodanig op- of aanmerkingen te maken.
Het OM maakt evenwel van de gelegenheid gebruik om aandacht te vragen voor het feit dat de computerdelicten verspreid over het Wetboek van Strafrecht (verder: Sr) geregeld zijn. Aanbevolen wordt om – bij een daarvoor geschikte gelegenheid – één titel in het Wetboek te creëren, waarin alle strafbepalingen met betrekking tot cybercriminaliteit bij elkaar worden ondergebracht.
Met het OM ben ik van mening dat een dergelijke exercitie het bestek van dit wetsvoorstel, dat enkel ziet op de implementatie van een richtlijn, te buiten gaat. Daarnaast teken ik daarbij aan, dat de wenselijkheid van een afzonderlijke titel in het Wetboek van Strafrecht nog een nadere afweging vergt. Voor de huidige plaatsing van de artikelen pleit dat is aangesloten bij de gepleegde gedraging. Zo is het wederrechtelijk binnendringen van een computer (artikel 138ab Sr) geplaatst bij de overige bepalingen over wederrechtelijk binnendringen en het artikel over de vernieling van computergegevens (art. 350 Sr) bij de overige bepalingen over vernieling.

De NVvR heeft bij bestudering van het wetsvoorstel en de reeds bestaande Nederlandse wetgeving geen hiaten aangetroffen.
Naar aanleiding van de adviezen van de NVvR en de Rvdr zijn de begrippen «botnet» en «vitale infrastructuur» in paragraaf 3 van deze memorie van toelichting nader verduidelijkt.
Eveneens is naar aanleiding van het advies van de NVvR in de inleiding van deze memorie toelichting een passage opgenomen over de opsporing van computercriminaliteit.

De Rvdr heeft in het wetsvoorstel geen aanleiding gezien tot het maken van inhoudelijke opmerkingen. Wel heeft de Rvdr enkele opmerkingen van juridisch-technische aard, opgenomen in de bijlage bij het advies. De Rvdr vraagt er aandacht voor dat een aantal van de reeds bestaande nationale bepalingen waarmee de richtlijn wordt geïmplementeerd, een breder bereik heeft dan de bepalingen in de richtlijn. De Rvdr noemt in dit verband artikel 3 van de richtlijn en artikel 138ab Sr en artikel 10 van de richtlijn ten aanzien van rechtspersonen. Naar aanleiding hiervan merk ik op dat het inderdaad zo is dat de bestaande wettelijke bepalingen een ruimere bescherming bieden. Omdat de gedragingen ten aanzien van het

[2] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

doorbreken van een beveiligingsmaatregel genoemd in de richtlijn onder de delictsomschrijvingen van die bepalingen vallen, is daarmee reeds aan de implementatieverplichtingen voldaan. Overigens verplicht de richtlijn er, anders dan de Rvdr lijkt te veronderstellen, niet toe rechtspersonen *strafrechtelijk* aansprakelijk te stellen. Dat is aan de lidstaten zelf. Op de overige technische opmerkingen van de Rvdr zal in paragraaf 3 bij de desbetreffende artikelen nader worden ingegaan. Naar aanleiding van het advies zijn verder enkele verhelderingen aangebracht in deze memorie van toelichting.

2. Hoofdlijnen wetsvoorstel

Voor een groot deel voldoet Nederland al aan hetgeen waartoe de richtlijn verplicht.
In de jaren negentig van de vorige eeuw is het Wetboek van Strafrecht uitgebreid met bepalingen die specifiek zijn toegespitst op strafbare feiten gepleegd door middel van of met betrekking tot geautomatiseerde werken (de Wet computercriminaliteit, Stb. 1993, 33). De Wet computercriminaliteit II (Stb. 2006, 300) bouwde hierop voort. Met die wet werden het Cybercrimeverdrag en het kaderbesluit uit 2005 – waar de richtlijn, zoals in paragraaf 1 reeds aan de orde kwam, een grote overlap mee vertoont – geïmplementeerd.
Anders dan in het Cybercrimeverdrag, het kaderbesluit en de richtlijn, waar de strafbare gedragingen bij elkaar zijn geplaatst, zijn de strafbaarstellingen van de verschillende vormen van computercriminaliteit verspreid over het Wetboek van Strafrecht opgenomen om deze te kunnen inpassen in de bestaande structuur van dat wetboek. Het betreft in de eerste plaats de computervredebreuk (artikel 138ab Sr) en de strafbaarstelling van ernstige «spam» of «bombing» (artikel 138b Sr), die staan opgenomen in de Titel over de misdrijven tegen de openbare orde (Boek II, Titel V). Ook de bepalingen uit die Titel over het aftappen of opnemen van gegevens (artikelen 139ba tot en met 139e Sr) zijn relevant, voor zover het gaat om het aftappen en opnemen van computergegevens. Daarnaast gaat het om de artikelen 161sexies en 161septies Sr, waarin de vernieling etc. van geautomatiseerde werken en werken voor telecommunicatie is strafbaar gesteld. Deze bepalingen zijn opgenomen in Boek II, Titel VII, misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht. Verder kan nog gewezen worden op artikel 326c Sr, het listiglijk gebruikmaken van telecommunicatiediensten, ondergebracht in Titel XXV van Boek II over bedrog. Ook Boek II, Titel XXVII, over vernieling, bevat enkele computermisdrijven. Het betreft de artikelen 350a en 350b (beschadiging van computergegevens), en 351 en 351bis Sr (beschadiging van werken ten algemenen nutte), voor zover betrekking hebbend op geautomatiseerde werken.
Tot slot valt een aantal gedragingen ook binnen de termen van commune delicten, zoals valsheid in geschrift (artikelen 225 en 226 Sr) en vernieling (artikel 350 Sr).

Met bovengenoemde bepalingen is het grootste deel van de gedragingen, omschreven in de richtlijn, reeds strafbaar gesteld. Alleen artikel 9 van de richtlijn behoeft nog in wetgeving geïmplementeerd te worden. Dat artikel bevat enkele bepalingen over de minimale maximumstraffen die op de verschillende gedragingen moeten worden gesteld. Implementatie van dit artikel leidt tot een verhoging van de strafmaat van enkele in het Wetboek van Strafrecht opgenomen computermisdrijven naar een maximale gevangenisstraf van twee jaar. Daarnaast worden ten behoeve van de implementatie van artikel 9 van de richtlijn drie strafverzwarende omstandigheden geïntroduceerd. De maximaal op te leggen gevangenisstraf zal worden verhoogd naar drie jaar wanneer gebruik wordt gemaakt van een «botnet», en naar vijf jaar wanneer het strafbare feit ernstige

schade ten gevolge heeft of wanneer het feit is gepleegd tegen een geautomatiseerd werk van een vitale infrastructuur.

3. Inhoud richtlijn en wijze van implementatie

Artikel 1 van de richtlijn omschrijft het onderwerp van de richtlijn. Deze bepaling behoeft naar haar aard geen implementatie.

Artikel 2 van de richtlijn bevat de definities van enkele in de richtlijn voorkomende begrippen. De definities komen overeen met de definities in artikel 1 van het kaderbesluit. De richtlijn verplicht er niet toe om de definities (al dan niet letterlijk) over te nemen in de nationale wetgeving. In het Wetboek van Strafrecht zijn de termen «gegevens» (artikel 80quinquies Sr) en «geautomatiseerd werk» (artikel 80sexies Sr) zodanig gedefinieerd dat daarmee volstaan kan worden voor wat betreft de definities van «computergegevens» (artikel 2, onder b, van de richtlijn) respectievelijk «informatiedragers» (artikel 2, onder a, van de richtlijn). Met de aanvaarding en inwerkingtreding van het wetsvoorstel tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III) – waarover de Afdeling advisering van de Raad van State recentelijk advies heeft uitgebracht – wordt de definitie van «geautomatiseerd werk» in artikel 80sexies aangepast. Daarbij wordt die bepaling terminologisch meer in lijn gebracht met de definitie van «informatiesysteem» uit de richtlijn. De aldaar voorgestelde wijziging van artikel 80sexies heeft derhalve geen gevolgen voor dit wetsvoorstel.
Hetgeen onder het begrip «rechtspersoon» (artikel 2, onder c, van de richtlijn) wordt verstaan, volgt reeds uit de artikelen 2:1 e.v. van het Burgerlijk Wetboek en artikel 51 Sr. Het begrip «onrechtmatigheid» (artikel 2, onder d, van de richtlijn) is niet als zodanig gedefinieerd, maar is wel in de Nederlandse strafwetgeving verdisconteerd, doordat in de bepalingen in het Wetboek van Strafrecht waarin de gedragingen uit de richtlijn strafbaar zijn gesteld, de wederrechtelijkheid steeds als bestanddeel in de delictsomschrijving is opgenomen dan wel element van het strafbare feit is.

Artikel 3 van de richtlijn komt overeen met artikel 2 van het kaderbesluit en artikel 2 van het Cybercrimeverdrag. De bepaling uit de richtlijn verplicht de lidstaten tot het treffen van de nodige maatregelen om de opzettelijke en onrechtmatige toegang tot een informatiesysteem of een deel daarvan strafbaar te stellen wanneer het strafbare feit is gepleegd door doorbreking van een beveiligingsmaatregel. Deze gedraging is reeds strafbaar gesteld in artikel 138ab, eerste lid, Sr (computervredebreuk). Dat artikel stelt strafbaar het opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk of een deel daarvan. Van «binnendringen» is onder meer sprake indien de toegang tot het werk wordt verworven door het doorbreken van een beveiliging (zie artikel 138ab, eerste lid, onder a, Sr).

Artikel 4 van de richtlijn verplicht de lidstaten de nodige maatregelen te treffen om onrechtmatige systeemverstoringen strafbaar te stellen. De bepaling komt overeen met artikel 3 van het kaderbesluit en artikel 5 van het Cybercrimeverdrag. De in het artikel genoemde gedragingen zijn thans dan ook reeds strafbaar op grond van de artikelen 138b, 161sexies en 350a Sr.
Artikel 138b Sr stelt strafbaar het opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmeren door daaraan gegevens aan te bieden of toe te zenden («spam» of «bombing»).

Artikel 350a Sr stelt strafbaar het opzettelijk en wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens of andere gegevens toevoegen aan gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of worden overgedragen.
Het huidige artikel 161sexies, eerste lid, aanhef en onder 1°, Sr bepaalt dat de persoon die opzettelijk enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft indien daardoor wederrechtelijk verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens ten algemene nutte of stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een telecommunicatiedienst ontstaat. Deze strafbaarstelling wordt in dit wetsvoorstel overgeheveld naar een nieuw in te voegen artikel 350c Sr. Omdat de richtlijn de beperking tot gegevens «ten algemene nutte», zoals opgenomen in artikel 161sexies, eerste lid, onder 1°, niet stelt, wordt voorgesteld deze eis te laten vervallen. Hetzelfde geldt voor de eis dat het moet gaan om een *openbaar* telecommunicatienetwerk of een *openbare* telecommunicatiedienst. Door het komen te vervallen van deze delictsbestanddelen ligt verplaatsing van de inhoud artikel 161sexies, eerste lid, aanhef en onder 1°, Sr naar Boek II, Titel XXVII over vernieling in de rede, omdat dat artikelonderdeel daardoor inhoudelijk meer aansluit bij de artikelen 350a e.v. en 351 en 351bis Sr. De Rvdr onderschrijft, blijkens het advies, de verplaatsing van de inhoud van artikel 161sexies, eerste lid, onder 1° Sr naar een nieuw artikel 350c Sr. Naar aanleiding van de vraag van de Rvdr naar het komen te vervallen van het vereiste dat een telecommunicatienetwerk of -dienst openbaar is, merk ik op dat de reden daarvoor is dat niet uitgesloten is dat middels een telecommunicatienetwerk of -dienst, computergegevens als bedoeld in de richtlijn worden verwerkt, en de richtlijn, zoals gezegd, de eis van openbaarheid niet stelt.
Naar aanleiding van de opmerkingen in het advies van de Rvdr over de toepassing van de voorlopige hechtenis, is in dit wetsvoorstel een aanpassing van artikel 67, eerste lid, onder b, van het Wetboek van Strafvordering (verder: Sv) opgenomen. In dat artikelonderdeel wordt thans verwezen naar artikel 161sexies, eerste lid, onder 1°, en tweede lid, Sr. Nu de inhoud van die artikelleden wordt verplaatst naar de nieuw voorgestelde artikelen 350c en 350d Sr (zie ook de toelichting bij artikel 7 van de richtlijn hieronder), moet ook de verwijzing in artikel 67 Sv daarmee in overeenstemming worden gebracht.

Artikel 5 van de richtlijn komt overeen met artikel 4 van het kaderbesluit en artikel 4 van het Cybercrimeverdrag. De bepaling verplicht de lidstaten tot het treffen van de nodige maatregelen om onrechtmatige gegevensverstoring strafbaar te stellen. De in het artikel genoemde gedragingen zijn reeds strafbaar op grond van artikel 161sexies en 350a Sr. Hiervoor in de toelichting op artikel 4 van de richtlijn ben ik reeds ingegaan op de betekenis van deze strafbaarstellingen.

Artikel 6 van de richtlijn verplicht de lidstaten – net als in artikel 3, eerste volzin, van het Cybercrimeverdrag – om de nodige maatregelen te treffen om de onrechtmatige onderschepping van computergegevens strafbaar te stellen. De in artikel 6 van de richtlijn genoemde gedragingen zijn thans reeds strafbaar op grond van artikel 139c Sr, welk artikel bepaalt dat gestraft wordt de persoon die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk. Daarnaast is in dit verband nog relevant artikel 139d Sr, dat strafbaar stelt het op een bepaalde plaats aanwezig doen zijn van een technisch hulpmiddel, met

het oogmerk dat daardoor een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk wederrechtelijk wordt afgeluisterd, afgetapt of opgenomen. Anders dan de richtlijn biedt artikel 3, tweede volzin, van het Cybercrimeverdrag de mogelijkheid om als voorwaarde te stellen dat het feit wordt begaan met oneerlijke bedoelingen of betrekking heeft op een computersysteem dat met een ander computersysteem is verbonden. Omdat Nederland destijds geen gebruik heeft gemaakt van deze mogelijkheid, is geen nadere bijstelling van de delictsomschrijving nodig.

Artikel 7 van de richtlijn ziet op instrumenten voor het plegen van strafbare feiten. Het artikel verplicht de lidstaten tot het treffen van de nodige maatregelen om strafbaar te stellen het opzettelijk vervaardigen, verkopen, verkrijgen voor gebruik, invoeren, verspreiden of op andere wijze beschikbaar maken van a) een computerprogramma dat hoofdzakelijk is ontworpen of geschikt is gemaakt voor het plegen van de in de artikelen 3 tot en met 6 van de richtlijn bedoelde strafbare feiten of b) een computerwachtwoord, toegangscode of soortgelijke gegevens waarmee toegang kan worden gekregen tot een informatiesysteem of een deel daarvan. Eis voor strafbaarheid is volgens artikel 7 van de richtlijn dat een en ander opzettelijk geschiedt en met het oogmerk om de instrumenten te gebruiken voor het plegen van de in de artikelen 3 tot en met 6 van de richtlijn bedoelde feiten.
Artikel 7 van de richtlijn komt overeen met artikel 6, eerste lid, van het Cybercrimeverdrag. Het Cybercrimeverdrag biedt in aanvulling daarop nog de mogelijkheid om bij wet als voorwaarde voor de strafbaarheid te stellen dat sprake moet zijn van het bezit van een bepaald aantal van deze technische hulpmiddelen of gegevens. Van deze mogelijkheid tot begrenzing van de strafbaarstelling heeft Nederland destijds geen gebruikgemaakt, waardoor de huidige strafbaarstellingen geen verdere aanpassing behoeven.
De in artikel 7 van de richtlijn omschreven gedragingen beogen in wezen de strafbaarstelling van een aantal specifieke voorbereidingshandelingen. In algemene zin kan daarvoor voor de Nederlandse situatie worden verwezen naar de algemene voorbereidingsbepaling van artikel 46 Sr. In dat artikel gaat het om de voorbereiding van misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld. De bepaling kan derhalve van betekenis zijn voor computerdelicten die een hoog strafmaximum kennen, zoals het huidige artikel 161sexies, eerste lid, onder 3° en 4°. Daarnaast kent artikel 139d Sr de strafbaarstelling van een specifiek soort voorbereidingshandeling die ten deze relevant kan zijn: strafbaar is hij die een technisch hulpmiddel op een bepaalde plaats aanwezig doet zijn, met het oogmerk dat daardoor een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk wederrechtelijk wordt afgeluisterd, afgetapt of opgenomen. Tot slot is de Nederlandse strafwet destijds ter gelegenheid van de implementatie van het Cybercrimeverdrag aangevuld met een aantal specifieke bepalingen ter implementatie van artikel 6 van dat verdrag. Deze bepalingen omvatten daarmee ook reeds de gedragingen van het met die bepaling overeenkomende artikel 7 van de richtlijn. Het betreft de artikelen 139d, tweede lid, en 161sexies, tweede lid, Sr. Dit laatste artikellid wordt met dit wetsvoorstel – in verband met de verplaatsing van de inhoud van artikel 161sexies, eerste lid, onder 1°, naar het nieuw voorgestelde artikel 350c Sr – overgeheveld naar het nieuw voorgestelde artikel 350d Sr.

Artikel 8 van de richtlijn komt overeen met artikel 5 van het kaderbesluit en artikel 11 van het Cybercrimeverdrag. Artikel 8 verplicht tot de strafbaarstelling van de uitlokking van of medeplichtigheid aan een van de in de artikelen 3 tot en met 7 van de richtlijn genoemde feiten. Daarnaast

bevat het artikel de verplichting tot de strafbaarstelling van poging tot het plegen van de in artikel 4 en 5 van de richtlijn genoemde feiten.
Het Nederlandse strafrecht voorziet in een algemene regeling betreffende de strafbaarheid van uitlokking, medeplichtigheid en poging. Artikel 47, eerste lid, onder 2°, Sr bepaalt onder meer dat ook zij die het strafbare feit uitlokken als dader strafbaar zijn. Artikel 48 Sr stelt medeplichtigheid aan een misdrijf strafbaar. Poging tot een misdrijf is strafbaar gesteld in artikel 45 Sr. Ook de uitlokking, medeplichtigheid aan en poging tot computermisdrijven zijn aldus strafbaar.

Artikel 9 van de richtlijn ziet op het strafmaximum van de in de artikelen 3 tot en met 7 van de richtlijn opgenomen strafbare feiten. De verplichting om op de in deze artikelen omschreven computerdelicten een maximale gevangenisstraf van ten minste twee jaar te stellen en de bepalingen over strafverzwarende omstandigheden zijn nieuw ten opzichte van zowel het kaderbesluit als het Cybercrimeverdrag. Ter implementatie van artikel 9 worden derhalve enkele wijzigingen in het Wetboek van Strafrecht voorgesteld.
Artikel 9, eerste lid, van de richtlijn verplicht de lidstaten de nodige maatregelen te treffen om ervoor te zorgen dat op grond van de richtlijn strafbaar gestelde of te stellen feiten doeltreffende, evenredige en afschrikkende straffen worden gesteld. In de daarop volgende leden wordt dit nader ingekaderd.
Het tweede lid van artikel 9 verplicht tot het stellen van een maximale gevangenisstraf van ten minste twee jaar op de in de artikelen 3 tot en met 7 van de richtlijn bedoelde feiten. Ter implementatie van dit artikellid worden de strafmaxima in de artikelen 138ab, eerste lid, 138b, eerste lid, 139c, eerste lid, 139d, eerste lid, Sr verhoogd. Ook in het nieuwe artikel 350c Sr – waarnaar de inhoud van artikel 161sexies, eerste lid, onder 1°, wordt verplaatst – zal een strafmaximum van twee jaar worden opgenomen. Het strafmaximum van artikel 350a, eerste lid, Sr voorziet reeds in een strafmaximum van twee jaar.
In artikel 9, derde lid, van de richtlijn is de verplichting opgenomen een maximale gevangenisstraf van ten hoogste drie jaren te stellen op het begaan van onrechtmatige systeem- of gegevensverstoring in de artikelen 4 en 5 van de richtlijn met behulp van een groot aantal geautomatiseerde werken die getroffen zijn door het gebruik van a) een computerprogramma dat hoofdzakelijk geschikt is gemaakt voor het plegen van een van de in de artikelen 3 tot en met 6 van de richtlijn bedoelde strafbare feiten, of b) een computerwachtwoord, toegangscode of soortgelijke gegevens waarmee toegang kan worden verkregen tot een informatiesysteem of een deel daarvan. Het gaat, met andere woorden, om een strafverhoging wanneer gebruik wordt gemaakt van een «botnet». Bij een «botnet» wordt, zoals in de inleiding reeds aan de orde kwam, op afstand controle over een aanzienlijk aantal computers tot stand gebracht door deze door middel van gerichte cyberaanvallen te besmetten met kwaadaardige software. Als het eenmaal tot stand is gekomen, kan het netwerk van computers dat de «botnet» vormt, zonder medeweten van de gebruikers ervan, worden ingezet om een grootschalige cyberaanval uit te voeren, die ernstige schade kan veroorzaken. Ik verwijs ook naar overweging 5 van de richtlijn. Voorwaarde is dat het computerprogramma, computerwachtwoord, de toegangscode of de soortgelijke gegevens hoofdzakelijk geschikt zijn gemaakt of zijn ontworpen om het «botnet» te maken. Deze strafverzwarende omstandigheid zal worden opgenomen in de artikelen 138b, tweede lid, 350a, tweede lid en 350c, tweede lid, Sr.
Artikel 9, vierde lid, noemt drie gevallen waarin het strafmaximum gesteld op de strafbare feiten, genoemd in de artikelen 4 en 5 van de richtlijn, minimaal vijf jaar dient te zijn, te weten wanneer het strafbare feit is gepleegd in het kader van een criminele organisatie (onder a), wanneer

het feit ernstige schade tot gevolg heeft (onder b) en wanneer het strafbare feit is gepleegd tegen een informatiesysteem (geautomatiseerd werk) van een vitale infrastructuur (onder c). Onder «vitale 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, zoals energiecentrales, vervoersnetwerken, of overheidsnetwerken, en waarvan de verstoring of vernietiging in een lidstaat aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken. Ik verwijs naar overweging 4 van de richtlijn. Onderdeel a behoeft geen implementatie. Deelneming aan een criminele organisatie wordt thans bedreigd met een maximale gevangenisstraf van zes jaar; zie artikel 140 Sr. De onderdelen b en c worden geïmplementeerd door toevoeging van een derde lid aan artikel 138b Sr, dat in de artikelen 350a, tweede lid, en 350c, tweede lid, Sr van overeenkomstige toepassing wordt verklaard.
Het vijfde lid van artikel 9 van de richtlijn behoeft geen implementatie. Dat artikellid bepaalt dat het misbruik maken van persoonsgegevens van een andere persoon met het oogmerk het vertrouwen van een derde te winnen, waardoor de rechtmatige bezitter van de identiteit schade wordt berokkend, als een strafverzwarende omstandigheid moet worden beschouwd, tenzij deze omstandigheden reeds worden bestreken door een ander feit dat overeenkomstig het nationale recht strafbaar is.
In het Nederlandse strafrecht kunnen strafverzwarende omstandigheden op twee verschillende manieren worden verdisconteerd. In de eerste plaats kan op het gronddelict een adequaat strafmaximum worden gesteld dat voor het openbaar ministerie en de rechter ruimte biedt om bij de strafeis respectievelijk de straftoemeting rekening te houden met strafverzwarende omstandigheden. In de tweede plaats kunnen strafverzwarende omstandigheden afzonderlijk in de wet worden omschreven en worden voorzien van een hoger strafmaximum dan het gronddelict.
Artikel 9, vijfde lid, van de richtlijn laat in beginsel ruimte voor een uitwerking in de nationale wetgeving volgens welke het openbaar ministerie in de strafeis en de rechter bij de straftoemeting binnen het op het misdrijf gestelde strafmaximum in strafverzwarende zin rekening houdt met de in artikel 9 genoemde omstandigheden. Doordat in dit wetsvoorstel de strafmaxima van de basisdelicten zijn verhoogd, hebben het openbaar ministerie en de rechter meer ruimte gekregen om rekening te houden met de genoemde strafverzwarende omstandigheid. Daardoor is nadere implementatie van deze bepaling niet nodig. In het Nederlandse strafrecht wordt daarenboven aan deze richtlijnbepaling voldaan doordat de aldaar genoemde gedraging afzonderlijk strafbaar is gesteld in artikel 231b Sr. Dat artikel stelt strafbaar het opzettelijk en wederrechtelijk identificerende persoonsgegevens, niet zijnde biometrische persoonsgegevens, van een ander gebruiken met het oogmerk om zijn identiteit te verhelen of de identiteit van de ander te verhelen of misbruiken, waardoor uit dat gebruik enig nadeel kan ontstaan.

Artikel 10 van de richtlijn ziet, evenals artikel 8 van het kaderbesluit en artikel 12 van het Cybercrimeverdrag, op de aansprakelijkheid van rechtspersonen in verband met de door de richtlijn bestreken strafbare feiten. Artikel 11 van de richtlijn ziet, evenals artikel 9 van het kaderbesluit en artikel 13, tweede lid, van het Cybercrimeverdrag, op de sancties die aan rechtspersonen kunnen worden opgelegd. De strafrechtelijke aansprakelijkheid van rechtspersonen is geregeld in artikel 51 Sr. Regels over de aan rechtspersonen op te leggen sancties zijn opgenomen in de artikelen 51, tweede lid, en 23, zevende lid, Sr.

Artikel 12 van de richtlijn ziet op de mogelijkheid tot het uitoefenen van rechtsmacht ten aanzien van de in de richtlijn genoemde strafbare feiten. De bepaling komt overeen met artikel 10, eerste en tweede lid, van het kaderbesluit en behoeft geen nadere implementatie.

De artikelen 13 en 14 van de richtlijn bevatten voorschriften over het uitwisselen van statistische informatie en over het verder versterken van de justitiële samenwerking door lidstaten ertoe te verplichten snel – via het al bestaande 24/7 netwerk van contactpunten voor cybercrime (zie artikel 11 van het kaderbesluit) – te reageren op urgente informatieverzoeken.
Het in de inleiding reeds genoemde THTC van de Dienst Nationale Recherche van de Landelijke Eenheid van de Nationale Politie, dat onder sturing staat van het Landelijk Parket van het openbaar ministerie, functioneert als het 24/7 contactpunt voor andere lidstaten. Het THTC is zodanig georganiseerd dat binnen een kort tijdbestek informatie kan worden gegeven aan een andere staat. Daarnaast kan het THTC andere Staten helpen met het uitvoeren van opsporingsacties, zoals bijvoorbeeld bij het bevriezingsbevel volgens artikel 126ni van het Wetboek van Strafvordering.
Deze 24/7 contactfunctie van de politie is ingesteld bij de in de inleiding reeds genoemde wet computercriminaliteit II, waarmee het Cybercrimeverdrag en het kaderbesluit werden geïmplementeerd. Artikel 35 van het Cybercrimeverdrag en de toelichting daarop spreken van een voortdurend beschikbaar contactpunt voor onmiddellijke ondersteuning en een snelle respons na ontvangst. Er is geen minimum responstijd genoemd. De richtlijn schrijft thans voor dat binnen maximaal 8 uur na ontvangst van het verzoek tot bijstand aan de vragende partij wordt bericht of het verzoek om bijstand zal worden ingewilligd, alsmede de vorm en het tijdstip waarop dit naar verwachting zal gebeuren. Deze minimum responstijd voor een eerste reactie aan de aanvragende partij zal in het werkproces van het THTC worden opgenomen.
Artikel 14 van de richtlijn verplicht ertoe om te zorgen voor een systeem voor het registreren, aanmaken en verstrekken van statistische gegevens over de in de artikelen 3 tot en met 7 van de richtlijn bedoelde strafbare feiten. Daarbij moet ten minste het aantal strafbare feiten worden geregistreerd en het aantal personen dat is vervolgd en veroordeeld. Deze gegevens kunnen uit bestaande politie en justitieregistraties worden gehaald.

De artikelen 15 tot en met 18 van de richtlijn behoeven uit hun aard geen implementatie.

4. Financiële consequenties

De in de richtlijn genoemde feiten zijn thans reeds strafbaar naar Nederlands recht en worden reeds opgespoord, vervolgd en berecht. De richtlijn stelt voor bepaalde delicten een hogere (maximale) strafbedreiging voor. In Nederland zal dit geen (grote) financiële consequenties hebben. Voor het vervullen van de functie van 24/7 contactpunt en voor het verzamelen van (statistische) informatie over de in de richtlijn genoemde strafbare feiten worden de bestaande structuren, enerzijds de bestaande politiële en justitiële informatiesystemen, en anderzijds het THTC, benut. Er worden derhalve geen grote extra financiële lasten van dit wetsvoorstel verwacht. Eventuele financiële consequenties zullen worden opgevangen binnen de begroting van het Ministerie van Veiligheid en Justitie.

De Minister van Veiligheid en Justitie,
I.W. Opstelten

BIJLAGE

Transponeringstabel behorende bij de implementatie van richtlijn 2013/40/EU van het Europees parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van kaderbesluit 2005/222/JBZ van de Raad (PbEU L 218/8)

Artikel(lid) richtlijn	Artikel wetsvoorstel of bestaande wet- en regelgeving	Toelichting
Artikel 1		Deze bepaling behoeft uit haar aard geen implementatie.
Artikel 2, onder a	Artikel 80sexies Sr	
Artikel 2, onder b	Artikel 80quinquies Sr	
Artikel 2, onder c	Artikel 2:1 e.v. BW en artikel 51, derde lid, Sr	Het begrip rechtspersoon dient in de eerste plaats in de civielrechtelijke betekenis te worden opgevat (artikel 2:1 e.v. BW). Voorts heeft de strafwetgever een uitbreiding gegeven aan het begrip rechtspersoon in artikel 51, derde lid, Sr.
Artikel 2, onder d	Artikelen 138ab, 138b, 139c, 139d, 350a en 350c Sr	In de bepalingen in het Wetboek van Strafrecht die de in de artikelen 3 tot en met 6 van de richtlijn omschreven gedragingen strafbaar stellen is wederrechtelijkheid als bestanddeel in de delictsomschrijving opgenomen of is dat element van het strafbare feit.
Artikel 3	Artikel 138ab, eerste lid, Sr	
Artikel 4	Artikelen 138b en 350a Sr Artikel I, onder G, wetsvoorstel	
Artikel 5	Artikel 350a Sr Artikel I, onder G, wetsvoorstel	
Artikel 6	Artikelen 139c en 139d Sr	
Artikel 7	Artikel 139d Sr Artikel I, onder G, wetsvoorstel	
Artikel 8, eerste lid	Artikelen 47, eerste lid, onder 2°, en 48 Sr	
Artikel 8, tweede lid	Artikel 45 Sr	
Artikel 9, eerste lid		Aan de hoogte van de straffen worden nadere eisen gesteld in artikel 9, tweede tot en met vijfde lid, van de richtlijn; zie ook aldaar.
Artikel 9, tweede lid	Artikel 350a Sr Artikel I, onder A, B, C, D en G, wetsvoorstel	
Artikel 9, derde lid	Artikel I, onder B, F en G, wetsvoorstel	
Artikel 9, vierde lid, onder a	140 Sr	
Artikel 9, vierde lid, onder b	Artikel I, onder B, F en G, wetsvoorstel	
Artikel 9, vierde lid, onder c	Artikel I, onder B, F en G, wetsvoorstel	

Artikel(lid) richtlijn	Artikel wetsvoorstel of bestaande wet- en regelgeving	Toelichting
Artikel 9, vijfde lid	Kamerstukken I 2012/13, 333 352, A (voorgestelde artikel 231b Sr)	Het artikellid laat in beginsel ruimte voor een uitwerking in de nationale wetgeving volgens welke het openbaar ministerie in de strafeis en de rechter bij de straftoemeting binnen het op het misdrijf gestelde strafmaximum in strafverzwarende zin rekening houdt met de in artikel 9 genoemde omstandigheden. In het Nederlandse strafrecht wordt daarenboven aan deze richtlijnbepaling voldaan doordat de aldaar genoemde gedraging in het genoemde wetsvoorstel afzonderlijk strafbaar wordt gesteld.
Artikel 10	Artikel 51 Sr	
Artikel 11	Artikelen 51, tweede lid, en 23, zevende lid, Sr	
Artikel 12, eerste lid en tweede lid	Artikelen 2 en 5 Sr	Er is (onder andere) sprake van rechtsmacht op grond van artikel 2 Sr indien het strafbare feit (fysiek) vanuit Nederland gepleegd wordt of in Nederland zijn uitwerking vindt.
Artikel 12, derde lid		Deze bepaling vergt geen aanpassing in nationale wetgeving.
Artikel 13		Deze bepaling vergt geen aanpassing in nationale wetgeving.
Artikel 14		Deze bepaling vergt geen aanpassing in nationale wetgeving.
Artikelen 15 tot en met 19		Deze bepalingen behoeven uit hun aard geen implementatie.