De Netwerk en informatiebeveiligingsrichtlijn

Kalis, J.P.

J.P. Kalis[1]

De Netwerk en informatiebeveiligingsrichtlijn[2]

Computerrecht 2017/48

Als onderdeel van het beleid van de EU aangaande cybersecurity en het beschermen van kritieke infrastructuur is na lang onderhandelen de Netwerk- en informatiebeveiligingsrichtlijn (NIB-richtlijn) in 2016 in werking getreden. Dit artikel geeft een kritische bespreking van de richtlijn, waarbij wordt ingegaan op de meerwaarde van de richtlijn en de vraag wordt gesteld of kan worden verwacht dat het doel, te weten om cybersecuritywetgeving in de EU te harmoniseren, zal slagen.

1. Introductie

Het is een periode van grote veranderingen in de Europese wetgeving rond cybersecurity, de beveiliging van (persoons) gegevens,[3] de telecommunicatiewetgeving,[4] en tevens de beveiliging van netwerk- en informatiesystemen. Deze gebieden hebben alle raakvlakken met elkaar, met name het feit dat al deze wetgeving in grote mate draait om netwerk- en informatiesystemen. De NIB-richtlijn is in dit kader een belangrijke nieuwe richtlijn en staat in dit artikel centraal.

De NIB-richtlijn is op 17 mei 2016 formeel aangenomen, en is in werking getreden op 8 augustus 2016. De richtlijn stelt zelf de redenen waarom zij in het leven geroepen is. Vanwege de cruciale rol die netwerk- en informatiesystemen en -diensten spelen in de samenleving is de betrouwbaarheid en beveiliging ervan essentieel.[5] De richtlijn stelt dat de omvang, de frequentie en de gevolgen van beveiligingsincidenten toenemen. Dit vormt een bedreiging voor de economie en het gebruikersvertrouwen.[6] Netwerk- en informatiesystemen, en met name het internet, zijn van groot belang voor het realiseren van de interne markt en het vrij verkeer van personen, goederen en diensten. Doel van de richtlijn is het harmoniseren van beveiligingseisen betreffende netwerk- en informatiesystemen. Een gecoördineerde aanpak en voortschrijdende samenwerking tussen de EU lidstaten is hierbij van groot belang. De richtlijn bevat enkele belangrijke beveiligingsverplichtingen voor zowel private partijen en lidstaten en legt de nadruk op samenwerking en het delen van informatie. Het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (ENISA) zal een belangrijke rol spelen als raadgevende institutie.

Er is een drietal kwesties die zich aandienen bij het lezen van de nieuwe richtlijn. Deze zullen in dit artikel worden behandeld. Ten eerste is het, gezien het streven om een "hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie" te bewerkstelligen, goed om te bezien wat de richtlijn toe zal voegen. Ten tweede is het, gelet op de beoogde harmonisatie, merkwaardig dat aanbieders van publieke elektronische communicatienetwerken en -diensten[7] (evenals verleners van vertrouwensdiensten)[8] buiten het bereik van deze richtlijn worden gehouden.[9] Ten derde moet worden bezien of het aannemelijk is dat het doel van de richtlijn bereikt kan worden. Aangezien de richtlijn net nieuw is valt er weinig te zeggen over de effectiviteit en doeltreffendheid van de wetgeving, maar ik zal in dit artikel middels een analyse van het stuk toch proberen daar iets over te zeggen. Voordat deze vragen beantwoord worden volgt eerst een bespreking van de inhoud van de richtlijn, waar ook aandacht wordt besteed aan de achtergronden. Deze bespreking is essentieel om de bovenstaande vragen te kunnen beantwoorden.

2. De belangrijkste onderwerpen in de richtlijn

2.1 *Hoofdstuk I Algemene bepalingen*

De basis van de richtlijn, het verbeteren van de werking van de interne markt, wordt gegeven in de eerste zin van het eerste artikel. Artikel 1 lid 2 specificeert de vijf centrale doelstellingen. Deze zijn (a) de verplichting voor de lidstaten een nationale strategie te ontwikkelen; (b) de instelling van een samenwerkingsgroep; (c) de totstandkoming van een CSIRT's-Netwerk; (d) de vaststelling van beveiligings- en meldingseisen voor de relevante actoren; en (e) de verplichting voor de lidstaten om nationale bevoegde autoriteiten, centrale contactpunten en CSIRT's aan te wijzen. Deze punten worden nader uitgelegd.

De richtlijn streeft naar minimumharmonisatie. Dat wil volgens artikel 3 zeggen dat lidstaten de mogelijkheid hebben een hoger niveau van netwerk- en informatiebeveiliging na te streven dan volgens de richtlijn verplicht wordt.

1 J.P. (Pieter) Kalis is PhD Candidate telecommunicatierecht bij eLaw@Leiden aan de Universiteit Leiden.

2 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (*PbEU* 2016, L 194/1).

3 In de vorm van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), (*PbEU* 2016, L 119/1).

4 Zie bijvoorbeeld het voorstel voor een Richtlijn van het Europees Parlement en de Raad tot vaststelling van het Europees wetboek voor elektronische communicatie, COM(2016) 590 final; en de uitgelekte conceptversie van de e-Privacyverordening, bijvoorbeeld te vinden via www.privacynieuws.nl/nieuwsoverzicht/internationaal-nieuws/eu-en-ep-nieuws/18259-nieuwe-e-privacy-verordening-europese-telecommunicatiewet.html.

5 Zie overweging (1).

6 Zie overweging (2).

7 In de zin van Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronischecommunicatienetwerken en -diensten (kaderrichtlijn) (*PbEU* 2002, L 108/33).

8 In de zin van de Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*PbEU* 2014 L 257/73).

9 Zie overweging (7) en artikel 1 lid 3.

De richtlijn is in grote lijn gericht tot twee actoren. Dit zijn de aanbieders van essentiële diensten en de digitaledienstverleners. Een digitaledienstverlener is een rechtspersoon die een dienst aanbiedt "van de informatiemaatschappij, dat wil zeggen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht".[10] Een aanbieder van een essentiële dienst is een publieke of private entiteit die een dienst verleent die "van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten; […] afhankelijk [is] van netwerk- en informatiesystemen," en waarvoor een beveiligingsincident "aanzienlijke verstorende effecten" zal hebben voor de verlening van die dienst.[11] De richtlijn zet uiteen welke sectoren geschaard moeten worden onder de essentiële diensten. Dit zijn energie, vervoer, het bankwezen, de infrastructuur van de financiële markten, de gezondheidszorg, drinkwatervoorzieningen en digitale infrastructuur. Het is vervolgens de verantwoordelijkheid van de lidstaten om vast te stellen welke specifieke entiteiten onder de gegeven definities vallen. De digitaledienstverleners daarentegen hoeven niet verder gespecificeerd te worden, de richtlijn geldt voor alle entiteiten die onder de betreffende in bijlage III gegeven soorten[12] vallen. Artikel 5 omschrijft alle criteria voor deze identificatie. In sommige sectoren is de identificatie van aanbieders al verder dan in andere sectoren. De financiële sector bijvoorbeeld is al zeer geharmoniseerd op Unie-niveau.
Samengevat worden de criteria voor de identificatie van aanbieders van essentiële diensten gegeven in artikel 5 lid 2: (a) een entiteit verleent een dienst die van essentieel belang is voor maatschappelijke en economische activiteiten; (b) die afhankelijk is van netwerk- en informatiesystemen; en (c) waarvoor een incident een aanzienlijke verstorende effecten zou hebben. Artikel 6 legt vervolgens uit wat met dat laatste bedoeld wordt.

Eén van de hoofdpunten van de richtlijn is dat er specifieke beveiligingseisen worden gesteld voor aanbieders van essentiële diensten en digitaledienstverleners. Twee punten zijn hierbij van belang. Ten eerste hebben deze eisen alleen betrekking op de beveiliging van de netwerk- en informatiesystemen van deze actoren. Het gaat dus niet om beveiliging van andere onderdelen van hun bedrijfsvoering. Ten tweede gaat het niet alleen om beveiliging tegen kwaadwillende aanvallen, maar tegen alle soorten incidenten die aanzienlijke gevolgen kunnen hebben voor de dienstverlening.

Zoals gebruikelijk worden nog enkele belangrijke definities gegeven. Allereerst de definitie van netwerk- en informatiesysteem in artikel 4 lid 1. Deze luidt als volgt:

> "a) een elektronisch communicatienetwerk in de zin van artikel 2, onder a), van Richtlijn 2002/21/EG; b) een apparaat of groep van geïnterconnecteerde of bij elkaar behorende apparaten, waarvan een of meer, overeenkomstig een programma, digitale gegevens automatisch verwerkt of verwerken, of c) digitale gegevens die via in de punten a) en b) bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan."

Meteen valt op dat het eerste onderdeel van de definitie die van een elektronisch communicatienetwerk is. Zoals eerder vermeld vallen dergelijke netwerken nu juist buiten de werking van de richtlijn. Deze contradictie zal verderop in het artikel besproken worden. Een voorbeeld van andere netwerk- en informatiesystemen onder b) kan zijn de ICT infrastructuur van een bank of een ziekenhuis.

De definitie voor beveiliging van netwerk- en informatiesystemen wordt gegeven in artikel 4 lid 2. Deze luidt als volgt:

> "Het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen."

Overweging (3) geeft aan dat "acties" breed moet worden opgevat om ook niet-opzettelijke gebeurtenissen te omvatten. Hoewel de beveiligingseisen zijn afgeleid van vergelijkbare beveiligingseisen die zijn neergelegd in de richtlijn gegevensbescherming[13] en het Europese telecommunicatierecht,[14] werd daar nog geen algemene definitie gegeven. Daarnaast geeft deze definitie aan dat het vooral de gegevens zijn die beschermd moeten worden. Het is daarbij van belang deze richtlijn niet te verwarren met de Algemene verordening gegevensbescherming, die zich richt op persoonsgegevens. Het betreft hier alle gegevens van netwerk- en informatiesystemen.

2.2 *Hoofdstuk II Nationale strategie, bevoegde autoriteiten en centraal contactpunt*

Hoofdstuk II bevat de verplichtingen voor lidstaten op nationaal niveau. Onderwerpen zijn onder meer het ontwikkelen van een nationale strategie voor de beveiliging van

10 Zie de NIB-richtlijn, artikel 4 lid 6 jo. lid 5; en Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (codificatie), (*PbEU* 2015, L 241/1), artikel 1 lid 1 sub b.

11 Zie de NIB-richtlijn, artikel 4 lid 4 jo. artikel 5 lid 2.

12 Dit zijn de onlinemarktplaats, de onlinezoekmachine en de cloudcomputerdiensten.

13 Zie artikel 17 van Richtlijn 95/46/E.G. van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEU* 1995, L 281/31).

14 Zie artikelen 13bis en 13ter van de Richtlijn 2009/140/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten, Richtlijn 2002/19/EG inzake de toegang tot en interconnectie van elektronische communicatienetwerken en bijbehorende faciliteiten, en Richtlijn 2002/20/EG betreffende de machtiging voor elektronische communicatienetwerken en -diensten (*PbEU* 2009, L 337/37).

netwerk- en informatiesystemen (artikel 7), het aanwijzen van nationale bevoegde autoriteiten en een centraal contactpunt (artikel 8), het aanwijzen van computer security incident response teams (CSIRT's) (artikel 9) en samenwerking op nationaal niveau (artikel 10).

Een nationale strategie helpt volgens de richtlijn de lidstaten een hoog niveau van netwerk- en informatiebeveiliging te bewerkstelligen op nationaal niveau. De nationale bevoegde autoriteiten controleren de uitvoering van de richtlijn op nationaal niveau. Het centrale contactpunt is er om grensoverschrijdende samenwerking en communicatie te faciliteren tussen nationale autoriteiten, de samenwerkingsgroep en het CSIRT's-netwerk. Zoals blijkt uit hoofdstukken IV en V hebben de nationale bevoegde autoriteiten enkele bevoegdheden om bindende instructies uit te vaardigen.

Alle sectoren van essentiële diensten moeten gedekt zijn door één of meerdere CSIRT's. Deze moeten effectief om kunnen gaan met beveiligingsrisico's en -incidenten. Teneinde nationale samenwerking te bevorderen, moeten de bevoegde nationale autoriteiten, de centrale contactpunten en de CSIRT's op nationaal niveau samenwerken om de doelstellingen van de richtlijn te realiseren. Meldingen van incidenten dienen te worden gedaan aan de bevoegde autoriteiten of de CSIRT's. Een samenvattend rapport betreffende dergelijke meldingen moet ieder jaar verstrekt worden aan de samenwerkingsgroep door het centrale contactpunt.

2.3 *Hoofdstuk III CSIRTs-netwerk en samenwerking op Unie-niveau*

Samenwerking tussen alle lidstaten is volgens de richtlijn van vitaal belang voor het bewerkstelligen van een hoog niveau van netwerk- en informatiebeveiliging, en een betrouwbaar gelijk speelveld. Artikel 11 schrijft de oprichting voor van een samenwerkingsgroep die zal bestaan uit vertegenwoordigers van de lidstaten, de Commissie en het ENISA. Haar taken zullen bestaan uit het ondersteunen en faciliteren van samenwerking en de uitwisseling van informatie, en daarmee het scheppen van vertrouwen. Zij moet samenwerken met relevante instituties, instellingen en organen van de Unie, alsook met de rechtshandhavingsautoriteiten, en daarmee bestaande informatiekanalen en gevestigde netwerken respecteren. De samenwerkingsgroep mag geen bindende verplichtingen opleggen.

Gezien het feit dat de meeste netwerk- en informatiesystemen in privaat eigendom zijn, is publiek-private samenwerking cruciaal. Daarom worden aanbieders van essentiele diensten en de samenwerkingsgroep aangemoedigd om samen te werken met de relevante partijen.
Artikel 12 omschrijft de instelling van een CSIRT-netwerk. Net als bij de samenwerkingsgroep is het doel het bijdragen aan het scheppen van vertrouwen. Het CSIRT-netwerk zal bestaan uit vertegenwoordigers van de CSIRT's van de lidstaten en CERT-EU,[15] met hulp van het ENISA. Het CSIRT-netwerk zal zich toeleggen op het delen van informatie en geleerde lessen, het verlenen van bijstand, en het uitvaardigen van richtsnoeren. Het CSIRT-netwerk mag geen bindende besluiten uitvaardigen.

2.4 *Hoofdstuk IV en V De beveiligingseisen en de meldingsverplichtingen*

De beveiligingseisen voor aanbieders van essentiële diensten en digitaledienstverleners in de richtlijn zijn conceptueel vergelijkbaar met de beveiligingseisen van Richtlijn 2002/21/EG en verordening 910/2014.[16] De beveiligingseisen zijn in principe een combinatie van drie elementen. Dit zijn ten eerste de verplichting tot het nemen van 'passende en evenredige technische en organisatorische maatregelen' ter beheersing van de risico's voor de beveiliging van netwerk- en informatiesystemen die zij bij hun activiteiten gebruiken. Het niveau van de maatregelen wordt gewogen naar vergelijk met de stand der techniek en de risico's die zich voordoen. Ten tweede dienen passende maatregelen genomen te worden om de gevolgen van beveiligingsincidenten te voorkomen en te minimaliseren teneinde de continuïteit van de diensten te waarborgen. Tenslotte moeten incidenten met aanzienlijke gevolgen voor deze continuiteit aan de bevoegde autoriteit of de CSIRT gemeld worden. Bij grensoverschrijdende gevolgen worden getroffen lidstaten eveneens op de hoogte gesteld. Omdat de maatschappelijke en economische risico's voor aanbieders van essentiële diensten groter zijn dan voor digitaledienstverleners, zijn de verplichtingen voor de laatste wat minder stringent.

Bij digitaledienstverleners kunnen de bevoegde autoriteiten enkel achteraf toezichtmaatregelen nemen wanneer er bewijs is dat deze dienstverleners niet aan hun verplichtingen voldoen. In het geval van aanbieders van essentiële diensten hebben de bevoegde autoriteiten de mogelijkheid om aanbieders te verplichten relevante informatie over hun beveiliging en bijbehorend beleid te overleggen, evenals bewijs daarvan. Wanneer er sector-specifieke regels van de Unie omtrent beveiligingseisen zijn opgenomen hebben deze bepalingen voorrang op de richtlijn, voor zover ze een in ieder geval gelijkwaardig niveau van bescherming bieden. Een voorbeeld dat genoemd wordt is dat van de bank- en financiële sector. Deze hebben al een hoog ontwikkeld beveiligingsregime.

De in de richtlijn gebruikte terminologie betreffende de beveiligingseisen laat veel ruimte over voor interpretatie. Voor de telecomsector heeft het ENISA enkele nuttige richtsnoeren uitgebracht over de implementatie van de beveiligings-

15 Het Computer Emergency Response Team for the EU institutions, bodies and agencies. Zie https://cert.europa.eu/cert/plainedition/en/cert_about.html.
16 Zie artikel 19 van Richtlijn 910/2014.

eisen.[17] Men mag verwachten dat deze richtsnoeren ook van nut kunnen zijn bij het implementeren van de verplichtingen in de richtlijn, in ieder geval totdat het ENISA richtsnoeren maakt in lijn met deze richtlijn. Hoewel niet specifiek genoemd in de hoofdstukken IV en V krijgt het ENISA een belangrijke algemene adviserende functie. Aangezien het ENISA inmiddels een belangrijke rol speelt bij het interpreteren van de beveiligingseisen en meldplichten in de telecomwetgeving is het aannemelijk dat dat in dit geval niet anders zal zijn.

2.5 *Hoofdstuk VI en VII Standaarden, vrijwillige melding en slotbepalingen*

Het zesde hoofdstuk bevat bepalingen betreffende standaardisering en vrijwillige meldingen. Om een uniforme implementatie van de richtlijn te bevorderen worden lidstaten aangemoedigd gebruik te maken van Europees of internationaal aanvaarde normen en specificaties. Hierbij wordt wel gesteld dat technologische neutraliteit daarbij gevolgd moet worden. Het ENISA zal hierbij een centrale rol spelen. Wanneer het openbaar belang gediend is mogen entiteiten die buiten de reikwijdte van deze richtlijn vallen beveiligingsincidenten vrijwillig melden, zolang dit geen onevenredige belasting voor de betrokken lidstaat is.

Het laatste hoofdstuk bevat de slotbepalingen, waaronder de boetebepalingen in artikel 21. Er worden geen specifieke voorschriften gegeven voor boetes, die moeten lidstaten zelf vaststellen. De Commissie moet uiterlijk op 9 mei 2018 van deze voorschriften op de hoogte gesteld worden.

Om een beter beeld te krijgen van waarom de richtlijn zo in elkaar zit als hierboven beschreven, worden de achtergronden van de richtlijn in de volgende paragraaf kort besproken.

3. De oorsprong van de NIB-richtlijn

3.1 *De informatiemaatschappij en de digitale economie*

Er zijn verscheidene startpunten aan te wijzen voor het proces dat heeft geleid tot de totstandkoming van de huidige NIB-richtlijn. Aan de ene kant bouwt de richtlijn voort op een lange lijn van beleidsstukken en wetgeving omtrent de zogeheten informatiemaatschappij en de digitale economie. Aan de andere kant lijkt het alsof de richtlijn, in ieder geval ten dele, het laatste woord is in de wetgeving betreffende de bescherming van kritieke infrastructuur.

Beleid rond de informatiemaatschappij werd het eerst vormgegeven door middel van een besluit van de Raad[18] ter ontwikkeling van strategieën voor de beveiliging van informatiesystemen. Dit concept vond een vervolg in het eEurope initiatief, dat werd gestart met een Mededeling van de Europese Commissie in 1999,[19] ter bevordering van de toegang tot het digitale tijdperk. De Mededeling spreekt van een verschuiving van een industriële maatschappij naar een nieuwe economie, die de informatiemaatschappij genoemd wordt. Het versterken van privacy en beveiliging alsmede de voortzetting van de liberalisering van de telecommunicatiemarkt worden genoemd als maatregelen om de informatiemaatschappij te bevorderen.

Uit het eEurope initiatief is in 2001 een eerste voorstel voor een Europese beleidsaanpak Netwerk- en informatieveiligheid[20] voortgekomen. Omdat in het verleden communicatienetwerken werden onderhouden door nationale monopolies was de beveiliging een wat meer eenduidige zaak. Liberalisering, convergentie en globalisering hebben dit veranderd. De redenen die gegeven werden voor interventie waren de volgende. Ten eerste waren er al beveiligingsverplichtingen in telecommunicatie en dataprotectie; ten tweede heeft de NIB-richtlijn ook invloed op de nationale veiligheid; en ten derde realiseerde men zich dat de markt de bestaande beveiligingsproblematiek niet uit zichzelf oploste.[21]

3.2 *Bescherming van kritieke infrastructuur*

Tot zover was de ratio achter netwerk- en informatiebeveiliging grotendeels economisch van aard. Kort na het verschijnen van de Mededeling die het voorstel voor een Europese beleidsaanpak Netwerk- en informatieveiligheid bevatte, voltrokken zich echter de aanslagen van 11 september 2001. Netwerk- en informatiebeveiliging, zeker voor zover het de bescherming van kritieke infrastructuur betrof, kreeg een nieuw fundament in de strijd tegen het terrorisme (en daarmee in zekere zin in (supra)nationale veiligheid). De identificatie van Europese kritieke infrastructuur gebeurde tegen de achtergrond van de aanslagen in de VS en die in Madrid in 2004.[22] In de volgende jaren verschoof de nadruk wat naar een breder scala aan bedreigingen en risico's maar terrorisme bleef centraal staan, zoals blijkt uit de beleidsdocumenten en wetgeving betreffende bescherming van Europese kritieke infrastructuur en kritieke informatie-infra-

17 Zie bijvoorbeeld de Technical Guideline on Incident Reporting, Version 2.1, October 2014, te vinden op www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting; en de Guideline on Security measures for Article 4 and Article 13a, Version 1.0 December 2014, te vinden op www.enisa.europa.eu/publications/guideline-on-security-measures-for-article-4-and-article-13a.

18 Besluit van de Raad van 31 maart 1992 betreffende de beveiliging van informatiesystemen, (*PbEG* 1992, L 123/19).

19 Mededeling van 8 december 1999 over een initiatief van de Commissie voor de buitengewone Europese Raad van Lissabon op 23 en 24 maart 2000: eEurope – Een informatiemaatschappij voor iedereen (COM(1999)687 def. – Niet verschenen in het Publicatieblad).

20 Mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's, Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak, COM(2001)298 definitief.

21 Voor meer informatie over dit onderwerp, zie bijvoorbeeld het rapport betreffende Security Economics and the Internal Market, te verkrijgen via www.enisa.europa.eu/publications/archive/economics-sec/.

22 Zie bijvoorbeeld de Mededeling van de Commissie aan de Raad en het Europees Parlement, Terreuraanslagen – preventie, paraatheid en reactie, COM(2004) 698 definitief.

structuur.[23] Ook de EUCyberbeveiligingsstrategie[24] (waarin de ontwikkeling van deze richtlijn een nieuwe impuls heeft gekregen) en de Richtlijn over aanvallen op informatiesystemen[25] noemen terrorismebestrijding als belangrijke grond. De essentiële diensten, zoals opgesomd in Bijlage II van de NIB-richtlijn, lijken te zijn afgeleid van de lijst van Europese kritieke infrastructuur zoals die is opgesteld in het voorstel voor de richtlijn ter inventarisatie van Europese kritieke infrastructuur.[26]

Het originele voorstel voor een netwerk- en informatiebeveiligingsrichtlijn uit 2013[27] noemt ook veel van de hier aangehaalde documenten specifiek als basis en stelt bescherming van kritieke infrastructuur centraal. In de uiteindelijke richtlijn is echter elke verwijzing naar kritieke infrastructuur of terrorisme verdwenen. Opnieuw is het functioneren van de interne markt de basis van de richtlijn. Incidenten die betrekking hebben op cybercrime worden verwezen naar de relevante rechtshandhavingsautoriteiten. De NIB-richtlijn werkt onverminderd de Richtlijn inzake de identificatie van Europese kritieke infrastructuur en de Richtlijn over aanvallen op informatiesystemen.

3.3 *De huidige positie van de NIB-richtlijn*

Thans valt het beleid betreffende de informatiemaatschappij onder de Strategie voor een digitaal eengemaakte markt voor Europa[28] (Digital Single Market Strategy ofwel DSM). Het doel is om het concept van de eengemaakte markt toe te passen op de digitale wereld, en hiervoor is het essentieel dat netwerk- en informatiesystemen open en goed beveiligd zijn. De NIB-richtlijn en de Algemene verordening gegevensbescherming zijn onderdeel van deze strategie.

4. Kritische reflectie

De doelstellingen van de netwerk- en informatiebeveiligingsrichtlijn, te weten het harmoniseren van beveiligingseisen en het stimuleren van samenwerking, zijn lovenswaardig. Gezien het enorme belang van netwerk- en informatiesystemen spelen in de huidige economie en samenleving is de bescherming ervan, zeker waar het gaat om essentiële diensten en belangrijke digitale diensten, van het grootste belang. De meerwaarde ligt in het feit dat een lappendeken aan wetgeving rond netwerk- en informatiebeveiligingswetgeving in de lidstaten op een minimumniveau wordt gebracht, en dat er beveiligingsnormen gaan gelden voor meer sectoren dan alleen de telecommunicatiesector en die een breder bereik hebben dan alleen gegevensbescherming. Daarnaast is het denken over beveiliging door de laatste jaren heen verschoven van reactief naar proactief. De realisatie dat beveiligingsincidenten nu eenmaal zullen gebeuren legt de nadruk meer op het leren omgaan met incidenten in plaats van het alleen maar proberen te voorkomen, en dat vindt zijn weerslag in deze richtlijn. Toch zijn er een aantal kanttekeningen te plaatsen.

Allereerst moet worden benadrukt dat de beveiligingseisen in deze richtlijn een veel groter bereik hebben dan kwaadwillige acties alleen. Wanneer men kijkt naar de Annual Incident Reports die ENISA eens per jaar uitbrengt over beveiligingsincidenten in de Europese telecomsector dan wordt dit duidelijk. Het meest recente rapport[29] stelt dat na analyse van de oorzaken van beveiligingsincidenten blijkt dat kwaadwillige acties minder dan drie procent van het totaal uitmaken. Als de telecomsector een leidraad mag zijn,[30] dan zal het overgrote deel van de beveiligingsincidenten veroorzaakt worden door systeemfouten, menselijke fouten en natuurverschijnselen. Dit alles nog los van het feit dat misdaadbestrijding buiten de reikwijdte van deze richtlijn valt. Bovendien was het te verwachten dat bescherming tegen terrorisme als grondslag voor deze richtlijn naar de achtergrond zou verdwijnen omdat netwerk- en informatiesystemen geen doel lijken te zijn van het internationale terrorisme, ook gezien het feit dat aanvallen op dergelijke systemen zo goed als niet voorkomen.
Het belang van deze richtlijn ligt erin dat netwerk- en informatiesystemen afdoende worden beveiligd, ongeacht wat de oorzaak van een beveiligingsincident is. Ook wordt meer gericht op het kunnen weerstaan van de consequenties van

23 Zie bijvoorbeeld het Groenboek betreffende een Europees programma voor de bescherming van kritieke infrastructuur, COM(2005) 576 definitief; de Mededeling van de Commissie betreffende een Europees programma voor de bescherming van kritieke infrastructuur, COM(2006) 786 definitief; het Voorstel voor een Richtlijn van de Raad inzake de inventarisatie van Europese kritieke infrastructuur, de aanmerking van infrastructuur als Europese kritieke infrastructuur en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuur te verbeteren, COM(2006) 787 definitief; de Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren (*PbEU* 2008, L 345/75); de Mededeling van de 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 "Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht", COM(2009) 149 definitief; en het Commission Staff Working Document on a new approach to the European Programme for Critical InfrastructureProtection, Making European Critical Infrastructures more secure, SWD(2013) 318 final.

24 Gezamenlijke Mededeling aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's Strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace, JOIN(2013) 1 final.

25 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* 2013, L 218/8).

26 Zie het Voorstel voor een Richtlijn van de Raad inzake de inventarisatie van Europese kritieke infrastructuur, de aanmerking van infrastructuur als Europese kritieke infrastructuur en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuur te verbeteren, COM(2006) 787 definitief, Bijlage I.

27 Voorstel voor een Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, COM(2013) 48 final.

28 Zie de Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, Strategie voor een digitale eengemaakte markt voor Europa, COM(2015) 192 final; en het Commission Staff Working Document A Digital Single Market Strategyfor Europe – Analysis and Evidence, SWD(2015) 100 final.

29 Te vinden op www.enisa.europa.eu/publications/annual-incident-reports-2015.

30 Ondanks het feit dat ze buiten het bereik van deze richtlijn gehouden worden, zijn electronische communicatienetwerken bij uitstek te beschouwen als netwerk- en informatiesystemen en kunnen deze cijfers goed als voorbeeld dienen op dit punt.

beveiligingsincidenten, in plaats van alleen het nemen van preventieve maatregelen.

Ten tweede is het opmerkelijk dat de richtlijn voor beveiligingseisen uit de telecommunicatiesector wordt uitgesloten. Richtlijn 2002/21/EG heeft reeds een regime met beveiligingseisen en dat is dan ook het argument electronische communicatienetwerken uit te sluiten van het bereik van de richtlijn.[31] Toch is dit frappant gezien het feit dat meerdere sectoren eveneens beveiligingseisen hebben. De richtlijn geeft dit zelf ook duidelijk aan.[32] Gezien het belang om juist de beveiligingseisen in (zeer) verschillende sectoren te harmoniseren doet vermoeden dat de belangen die de richtlijn wil behartigen er juist bij gebaat zouden zijn de telecommunicatiesector mee te nemen. Aan de kant van de beveiliging van persoonsgegevens en de telecommunicatiesector lijkt iets vergelijkbaars wel te gebeuren, wanneer men het voorstel voor een verordening betreffende privacy en elektronische communicatie[33] ziet. Voor de meeste beveiligingseisen wordt daarin doorverwezen naar de Algemene verordening gegevensbescherming.[34]

Een andere verklaring voor het uitsluiten van telecom kan worden gezocht in de verschillende achtergrond van de richtlijnen. Het feit dat bescherming tegen terrorisme en cybercriminaliteit lange tijd een belangrijke basis voor bescherming van kritieke infrastructuur en ICT is geweest, kan een reden zijn waarom deze richtlijn los wordt gezien van de telecomsector (die zich van oudsher vooral op het terrein van liberalisering van de telecommunicatiemarkt en mededingingsrecht begaf) en de regelgeving rond elektronische handtekeningen en vertrouwensdiensten. Dit ondanks het feit dat de beveiligingseisen erg veel gemeen hebben met elkaar. Inmiddels is er geen conceptuele reden om de twee niet onder een overkoepelend regime te vatten.

Ten derde is het de vraag of een richtlijn het juiste instrument is om een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie te bewerkstelligen. De keuze van richtlijn als instrument is ingegeven door de wens de verscheidene bestaande regelingen in de lidstaten intact te kunnen laten, en de lidstaten de mogelijkheid te bieden eigen reguleringen te maken. De richtlijn geeft aan dat bepaalde sectoren al reglementen hebben of gaan hebben, en dat daar ruimte voor moet zijn. Een verordening zou echter een hoger niveau van harmonisatie kunnen bewerkstelligen voor deze zeer belangrijke materie, in dezelfde mate als de algemene verordening gegevensbescherming dat doet. Een voorbeeld is de boetebedingen. Deze worden aan de lidstaten overgelaten, terwijl bijvoorbeeld de algemene verordening gegevensbescherming zelf duidelijke eisen stelt. Daarnaast is het maar de vraag of de vele entiteiten, die door deze richtlijn in het leven worden geroepen, daadwerkelijk effectief kunnen zijn, gezien de geringe macht die ze krijgen, bijvoorbeeld om bindende instructies te mogen geven.

5. Conclusie

Resumerend kan worden gesteld dat de richtlijn grote stappen gezet heeft in de Europese wetgeving betreffende de beveiliging van netwerk- en informatiesystemen, en het nut van de richtlijn is evident. Toch is het twijfelachtig of alle gestelde doelen kunnen worden bereikt met de richtlijn in zijn huidige vorm. Het verdient mijns inziens aanbeveling te onderzoeken of het mogelijk is op termijn toch voldoende politieke steun te krijgen om een verordening met dezelfde doelstelling te creëren, die ook de beveiligingsvereisten voor de telecomsector omvat, evenals een duidelijker boeteregime en meer bevoegdheden voor de centrale beveiligingsinstituties. Dit is echter een zaak die vooral op basis van het functioneren van de huidige richtlijn de komende jaren moet worden bekeken.

31 Zie overweging (7).
32 Zie overweging (9) e.v.
33 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.
34 Ibid., zie met name § 1.2 van het explanatory memorandum, op p. 2, en artikel 1 lid 3.