Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2017–2018

34 883 Regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen)

C

MEMORIE VAN ANTWOORD

Ontvangen 24 augustus 2018

Inleiding

Met belangstelling heb ik kennis genomen van het voorlopig verslag van de vaste commissie voor Justitie en Veiligheid over het wetsvoorstel houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen, hierna: Wbni). Graag maak ik van de gelegenheid gebruik om de gestelde vragen te beantwoorden en op enkele punten een nadere toelichting te geven. Bij de beantwoording heb ik de volgorde van het voorlopig verslag aangehouden. Waar dit de helderheid en overzichtelijkheid ten goede kwam, heb ik vragen samengenomen in de beantwoording.

Taken van de Minister van Justitie en Veiligheid

De Minister van Justitie en Veiligheid krijgt op grond van artikel 3, eerste lid, onder c, van het wetsvoorstel onder meer als taak het bijstaan van vitale aanbieders en van andere aanbieders die onderdeel zijn van de rijksoverheid bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen. De leden van de VVD-fractie vragen de regering wat het bijstaan precies inhoudt. Tot hoever reikt deze taak? Beperkt de Minister zich tot het geven van algemene adviezen en best practices? Of gaat de Minister ook individuele aanbieders bijstaan en van adviezen voorzien? Zal de Minister bijvoorbeeld ook ten behoeve van het uitbrengen van adviezen zogenaamde nulmetingen en andere assessments uitvoeren?

Met bijstaan, tevens de vervulling van de CERT-taak van het NCSC (Nationaal Cyber Security Centrum; CERT staat voor *computer emergency response team)*, wordt onder meer bedoeld het adviseren, waarschuwen, waar mogelijk geven van handelingsperspectief en anderszins ondersteunen bij concrete dreigingen en incidenten. Waar nodig staat het NCSC ook individuele aanbieders bij. Uiteraard blijven de betrokken aanbieders zelf primair verantwoordelijk voor het beveiligen van hun informatiesystemen. Het uitvoeren van nulmetingen en andere assessments door het

kst-34883-C
ISSN 0921 - 7371
's-Gravenhage 2018

NCSC ligt niet voor de hand. Aanbieders kunnen immers zelf dergelijke maatregelen treffen om inzicht te krijgen in hun beveiligingsniveau. Ook kan de bevoegde autoriteit (de sectorale toezichthouder) een aanbieder van een essentiële dienst (AED) verplichten om een onafhankelijke deskundige te laten onderzoeken of de door de AED genomen maatregelen voldoen aan de beveiligingseisen van de Wbni (beveiligingsaudit, zie artikel 26 Wbni). Ook kan de bevoegde autoriteit zelf bij een AED zo'n audit uitvoeren.

Verder vragen de genoemde leden wat het verschil is tussen een CSIRT en een computercrisisteam.

De term computercrisisteam (in de praktijk vaak een CERT genoemd) wordt in de Wbni (in navolging van de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc)) gebruikt voor elke instantie die tot taak heeft aanbieders te adviseren over digitale veiligheid en te helpen bij ICT-incidenten. De NIB-richtlijn introduceert de term CSIRT: computer security incident response team. Een CSIRT is altijd een CERT, maar niet elke CERT is een CSIRT. Elke lidstaat van de EU moet een of meer CSIRT's aanwijzen die voldoen aan de vereisten van bijlage I, onderdeel 1, van de richtlijn. CSIRT's zijn belast met de taken van onderdeel 2 van die bijlage. Nederland wijst twee CSIRT's aan: de Minister van Justitie en Veiligheid (het NCSC) wordt het CSIRT voor AED's en de Minister voor Economische Zaken en Klimaat (EZK) wordt het CSIRT voor digitaledienstverleners (DSP's).

Wat zijn de criteria om op de lijst van de ministeriële regeling te komen, zo vragen de leden van de VVD-fractie. En hoe wordt voorkomen dat een organisatie die niet op de lijst staat, maar wel voor een bepaalde sector of beroepsgroep vergelijkbare diensten verleent als die van een computercrisisteam, niet geïnformeerd wordt over dreigingen en incidenten?

Om toegevoegd te worden aan de lijst in de ministeriële regeling, bedoeld in artikel 3, tweede lid, onder c, Wbni, vindt er een toetsing plaats waarin moet worden vastgesteld dat uitwisseling van gegevens over dreigingen of incidenten verantwoord en gerechtvaardigd is. Criteria die daarbij onder meer gelden, zijn of voldoende is gebleken dat de organisatie gegevens op een zorgvuldige en rechtmatige wijze verwerkt, en dat delen van gegevens bijdraagt aan het voorkomen van nadelige gevolgen voor het maatschappelijk verkeer. Zo nodig kan een computercrisisteam na toetsing op korte termijn worden toegevoegd aan de lijst van de ministeriële regeling.

Meldplicht voor incidenten

De leden van de VVD-fractie merken op dat zorgaanbieders nu ook gekwalificeerd gaan worden als AED's.

In reactie hierop wijs ik erop dat het wetsvoorstel zelf geen AED's aanwijst. AED's en andere vitale aanbieders zullen worden aangewezen in of op grond van het Besluit beveiliging netwerk- en informatiesystemen (Bbni), een algemene maatregel van bestuur die zal worden vastgesteld op grond van artikel 5 Wbni. In bijlage II van de NIB-richtlijn wordt de gezondheidszorg genoemd als sector met potentiële AED's, met als deelsector zorginstellingen. Het is aan de lidstaten om te bepalen welke zorgaanbieders in hun land voldoen aan de criteria voor de aanwijzing van AED's in de artikelen 5, eerste lid, en 6 van de NIB-richtlijn. De regering heeft vooralsnog niet het voornemen om zorgaanbieders aan te

wijzen als AED.[1] Wel zal zij de lijst van AED's periodiek actualiseren, zoals de NIB-richtlijn ook voorschrijft (artikel 5, vijfde lid). Dat kan er dus toe leiden dat bepaalde zorgaanbieders in de toekomst alsnog in het Bbni worden aangewezen als AED. Mogelijk zijn de leden van de VVD-fractie op het verkeerde been gezet door artikel 4, eerste lid, van het wetsvoorstel, waarin de Minister voor Medische Zorg wordt aangewezen als de bevoegde autoriteit voor de sector gezondheidszorg. Die aanwijzing heeft tot doel om te voorkomen dat eerst de Wbni moet worden gewijzigd als de regering in de toekomst bepaalde zorgaanbieders alsnog in het Bbni wil aanwijzen als AED.

Verder vragen de leden van de VVD-fractie hoe wordt voorkomen dat aanbieders die bij verschillende instanties (CSIRT, bevoegde autoriteit en soms ook de Autoriteit persoonsgegevens (AP)) dezelfde meldingen moeten doen, op verschillende wijzen worden behandeld en hoe onnodige administratieve rompslomp voor deze aanbieders wordt voorkomen. De leden van de PvdA-fractie vernemen graag van de regering welke rol zij voor zichzelf ziet in het bevorderen van de samenwerking tussen de betrokken autoriteiten, ook gezien de overlap tussen de beveiligingseisen en meldplichten van de Algemene verordening gegevensbescherming (AVG) en de Wbni.

Iedere instantie waarbij gemeld moet worden heeft eigen taken en zal enkel informatie opvragen die voor de uitvoering van die taken nodig is. Aangezien de taken verschillen, is het onvermijdelijk dat meldingen op verschillende wijzen worden behandeld. Het CSIRT heeft als taak reageren op incidenten (advies en bijstand) en zorgen voor een dynamische risico- en incidentanalyse. Voor het uitvoeren van deze taak is andere informatie nodig dan de bevoegde autoriteit gebruikt voor het zorgdragen voor de bestuursrechtelijke handhaving van de wet of de AP gebruikt voor het handhaven van de AVG.
De regering bevordert de samenwerking en afstemming van werkwijzen tussen het CSIRT en de bevoegde autoriteiten in een werkgroep die maandelijks op het Ministerie van Justitie en Veiligheid bijeenkomt.
De regering wil de meldprocessen van de verschillende meldplichten van de Wbni zo veel mogelijk op elkaar afstemmen om onnodige administratieve lasten te voorkomen. De betrokken instanties zullen later dit jaar besluiten of het (technisch) mogelijk is dat initiële meldingen binnen de Wbni gedaan kunnen worden door één handeling. Specifiek voor DSP's wordt de mogelijkheid van één loket onderzocht. Hierbij moet wel wetgeving over verstrekken van informatie aan derden, zoals de artikelen 21 en 22 Wbni, in acht worden genomen.
In een volgend stadium zal worden onderzocht of stroomlijning met andere verplichte meldingen, zoals die bij de AP, wenselijk en haalbaar is. Dit is afhankelijk van de mate waarin er overlap is van te verstrekken gegevens tussen verschillende cybersecurity-gerelateerde meldplichten zoals die bij de AP.

In de wet zijn vier categorieën «bevoegde autoriteit» opgenomen. Niet (alle incidenten van) alle aanbieders zullen in een specifieke categorie vallen. Hoe en bij wie moeten deze overige aanbieders hun incidenten melden, zo vragen de leden van de VVD-fractie.

De in artikel 4, eerste lid, Wbni bedoelde aanwijzing van de bevoegde autoriteit ziet alleen op AED's, dus alleen op de essentiële diensten, aangewezen bij of krachtens het Bbni. De meldplicht ziet alleen op

[1] Zie p. 30 van de memorie van toelichting (Kamerstukken II 2017/18, 34 883, nr. 3) en de brief van 2 juli 2018 van de Minister voor Medische Zorg aan de Tweede Kamer, Kamerstukken 2017/18, 27 529, nr. 158.

ernstige ICT-incidenten met betrekking tot die essentiële diensten. Dergelijke incidenten moeten gemeld worden bij de bevoegde autoriteit en bij het NCSC. Andere incidenten hoeven door AED's niet gemeld te worden. Voor DSP's geldt iets vergelijkbaars: de aanwijzing van de Minister van EZK als de bevoegde autoriteit geldt alleen voor de digitale diensten, bedoeld in bijlage III bij de NIB-richtlijn (onlinemarktplaatsen, onlinezoekmachines en cloudcomputerdiensten). De meldplicht geldt alleen voor ernstige ICT-incidenten met betrekking tot die diensten. Dergelijke incidenten moeten gemeld worden bij de bevoegde autoriteit en bij het in artikel 4, tweede lid, onder b, Wbni bedoelde CSIRT voor digitale diensten. Andere incidenten hoeven door DSP's niet gemeld te worden.

De leden van de PvdA-fractie vragen of de regering hun mening deelt dat voor de meldplicht de aard van een aanval of inbreuk minder een criterium van invloed zou moeten zijn, en de nadruk zou moeten liggen op de gevolgen van de ICT-inbreuk. Is de regering bereid om DDoS-aanvallen op te nemen in de meldplicht?

Ja, de regering deelt die mening. De nadruk bij de meldplicht van de Wbni ligt op de gevolgen van een aanval of inbreuk. De artikelen 10, eerste lid, onder a, en 13, eerste lid, zien op incidenten «met aanzienlijke gevolgen voor de continuïteit» van de dienst». DDoS-aanvallen vallen nu niet onder de meldplicht van de Wgmc, maar kunnen wel onder de meldplicht van de Wbni vallen, namelijk als een DDoS-aanval aanzienlijke gevolgen heeft voor de continuïteit van de dienst.

De leden van de PvdA-fractie vragen of de regering hun mening deelt dat de aansprakelijkheid door het doen van de melding niet mag toenemen.

Ja, de regering deelt die mening. De NIB-richtlijn bepaalt dat ook met zo veel woorden: «Melding leidt voor de meldende partij niet tot een verhoogde aansprakelijkheid» (artikel 14, derde lid, laatste volzin (AED's), en artikel 16, derde lid, laatste volzin (DSP's)).

Verwerking van gegevens

De leden van de PvdA-fractie constateren dat het NCSC de bevoegdheid krijgt om eenieder te verzoeken om gegevens te verstrekken. Zij merken op dat ontvangers van het verzoek weliswaar niet verplicht zijn mee te werken, maar daar mogelijk niet van op de hoogte zijn en zich toch verplicht voelen om mee te werken. Hoe denkt de regering dat te voorkomen?

Voor een goede taakuitoefening door het NCSC is het van belang dat het NCSC over voldoende gegevens beschikt over incidenten en kwetsbaarheden met betrekking tot informatiesystemen van de rijksoverheid en vitale private partijen. Het kan daarbij ook gaan om persoonsgegevens zoals IP-adressen. Artikel 18 Wbni biedt organisaties die persoonsgegevens willen delen met het NCSC een grondslag om dat op basis van dit artikel te doen. Het NCSC zal alleen gebruikmaken van de mogelijkheid om gegevens op te vragen op basis van dit artikel als dat noodzakelijk is voor de uitoefening van zijn wettelijke taken. In schriftelijke verzoeken en aan partijen die daarover vragen hebben, zal worden meegedeeld dat het delen van informatie op vrijwillige basis is. Ook zal hieraan op de website van het NCSC aandacht worden besteed. Overigens is er tot op heden bij organisaties nog geen onduidelijkheid geweest over het vrijwillige karakter van artikel 4 Wgmc, dat dezelfde strekking heeft als artikel 18 Wbni.

Openbaarmaking van incidenten

De bevoegde autoriteit kan ex artikel 23 incidenten openbaar maken als publieke bewustwording nodig is om incidenten te voorkomen of het publiek te informeren over een gemeld incident. De vitale aanbieder wordt weliswaar geraadpleegd, maar heeft uiteindelijk geen doorslaggevende stem. Welke rechtsbescherming heeft deze vitale aanbieder, zo vragen de leden van de VVD-fractie? De vitale aanbieder zal mogelijk bezwaar en beroep kunnen instellen, maar deze hebben geen schorsende werking. Openbaarmaking kan voor deze aanbieders echter wel schadelijke gevolgen hebben. Denk alleen al aan de mogelijke reputatieschade. Welke instrumenten hebben deze aanbieders op het moment dat ze het niet eens zijn met het besluit van een bevoegde autoriteit om een melding openbaar te maken? En zal de mogelijke openbaarmaking niet drempelverhogend werken voor aanbieders om meldingen bij de bevoegde autoriteiten te doen? Welke maatregelen treft de regering om het mogelijke negatieve effect van de mogelijke openbaarmaking van een melding op de meldingsbereidheid te mitigeren?

Artikel 23 implementeert de NIB-richtlijn en geldt alleen voor essentiële diensten (onderdeel a) en digitale diensten (onderdeel b). De bepaling geldt dus niet voor alle vitale aanbieders.
Gezien de belangen van de betrokken AED of DSP en het negatieve effect dat openbaarmaking kan hebben op de meldingsbereidheid, maar ook om te voorkomen dat openbaarmaking de problemen niet gróter maakt, zal de bevoegde autoriteit terughoudend omgaan met het openbaarmaken van incidenten, vooral met het openbaarmaken van tot een AED of DSP herleidbare gegevens. De bevoegdheid van artikel 23 moet worden gelezen tegen de achtergrond van overweging 59 van de NIB-richtlijn: «De bevoegde autoriteiten moeten de nodige aandacht besteden aan de instandhouding van informele en betrouwbare kanalen voor informatie-uitwisseling. Bij de bekendmaking van aan de bevoegde autoriteiten gemelde incidenten moet het belang van het publiek om te worden geïnformeerd over bedreigingen worden afgewogen tegen mogelijke commerciële en imagoschade voor de aanbieders van essentiële diensten en digitaledienstverleners die incidenten melden. Bij het nakomen van de meldingsverplichtingen moeten de bevoegde autoriteiten en de CSIRT's bijzondere aandacht besteden aan de noodzaak om informatie over de kwetsbare punten van producten strikt vertrouwelijk te houden tot er passende herstel- en beveiligingsmaatregelen zijn genomen.»

Het bovenstaande brengt mee dat de bevoegde autoriteit bij de toepassing van artikel 23 slechts tot een AED of DSP herleidbare gegevens verstrekt voor zover:
1. verstrekking van herleidbare gegevens aan het publiek nodig is om een incident te voorkomen of een lopend incident te beheersen (AED's) of anderszins nodig is in het algemeen belang (DSP's),
2. het belang om het publiek te informeren opweegt tegen de belangen van de aanbieder, en
3. het informeren van het publiek de problemen naar verwachting niet gróter maakt.

Bij deze drie voorwaarden moet in elk geval worden meegewogen of met het verstrekken van herleidbare gegevens aan het publiek kan worden gewacht tot de aanbieder passende herstel- en beveiligingsmaatregelen heeft genomen.

Artikel 23 schrijft voor dat de bevoegde autoriteit niet eerder tot openbaarmaking overgaat dan na raadpleging van de betrokken AED of DSP. Bij dat overleg zal ook worden betrokken de vraag of de schade voor de

aanbieder kan worden beperkt als hij het publiek zelf informeert. De bevoegde autoriteit kan zo nodig vorderen dat de aanbieder dat doet.

Ik ga ervan uit dat tegen de beslissing tot openbaarmaking van tot een aanbieder herleidbare gegevens bestuursrechtelijke rechtsbescherming openstaat, gezien de grote belangen van de betrokken aanbieder. Inderdaad heeft het maken van bezwaar geen schorsende werking. In veel gevallen zal de bevoegde autoriteit kunnen wachten met de openbaarmaking van herleidbare gegevens tot de aanbieder de gelegenheid heeft gehad om de bestuursrechter om schorsing te vragen en die rechter dat verzoek heeft beoordeeld. Soms zal de spoedeisendheid van de situatie de bevoegde autoriteit dwingen tot acuut optreden. Hoe dan ook geldt dat de overheid aansprakelijk is voor de schade die wordt veroorzaakt door een onrechtmatig besluit tot openbaarmaking. Ook de wens om dat te voorkomen, zal eraan bijdragen dat de bevoegde autoriteit terughoudend omgaat met het openbaarmaken van tot een AED of DSP herleidbare incidentinformatie.

Een actieve openbaarmaking kan een effectieve bijdrage leveren aan bewustwording en verbetering van de bescherming van ICT-systemen. De leden van de **PvdA**-fractie vragen of de regering bereid is om transparantie te bieden over het aantal meldingen, type incidenten, de impact daarvan en de opvolging naar aanleiding van deze meldingen?

Ja, de instanties waarbij incidenten moet worden gemeld, zullen periodiek en op een geaggregeerd niveau informatie over de gemelde incidenten publiceren. Het gaat inderdaad om informatie zoals het aantal meldingen, soort incidenten, de duur van het incident, maar zonder vermelding van de individuele aanbieders.

Overlap tussen de beveiligingseisen en meldplichten van de AVG en het voorliggende wetsvoorstel

De vraag van de leden van de PvdA-fractie over het bevorderen van samenwerking tussen de betrokken autoriteiten is beantwoord in de paragraaf Meldplicht voor incidenten.

Onbekende kwetsbaarheden

Is de regering bereid, zo vragen de leden van de PvdA-fractie mede namens de leden van de fractie van de SP, te bewerkstelligen dat informatie over onbekende kwetsbaarheden die door onderzoekers, ethische hackers of anderen aan het NCSC wordt gemeld, altijd wordt doorgegeven aan de maker van de software waarin de onbekende kwetsbaarheid is gevonden, met uitzondering van die situaties waarin er naar het oordeel van het NCSC sprake is van een belang van nationale veiligheid?

Ja, als regel zal het NCSC informatie over een onbekende kwetsbaarheid doorgeven aan de maker van de software. Op die regel zijn uitzonderingen denkbaar, waaronder de situatie dat het belang van de nationale veiligheid eraan in de weg staat om de maker te waarschuwen, maar bijvoorbeeld ook als de maker kwade intenties heeft. Het NCSC zal hierbij altijd handelen in goed overleg met de melder.

Tot slot

De richtlijn moest uiterlijk op 9 mei 2018 geïmplementeerd zijn. Waarom is die datum niet gehaald, zo vragen de leden van de PvdA-fractie. Baart het de regering zorgen dat de Nederlandse invulling van de verplichtingen

van netwerk- en informatiebeveiliging, en daarmee de harmonisatie op Unieniveau, langer op zich zal laten wachten dan gewenst is?

De reden waarom Nederland de richtlijn niet op tijd volledig heeft omgezet, moet worden gezocht in de tijd die nodig is gebleken voor de totstandkoming van dit wetsvoorstel en de keuzes die daarvoor nodig waren. Samen met 16 andere lidstaten is Nederland inmiddels door de Europese Commissie in gebreke gesteld.[2] Wat betreft AED's eindigt de implementatietermijn overigens materieel een half jaar na 9 mei 2018. De termijn voor het aanwijzen van AED's verloopt namelijk op 9 november 2018. Zolang de AED's nog niet zijn aangewezen, kunnen de voor hen geldende bepalingen uiteraard nog niet in werking treden. Daarnaast wil ik erop wijzen dat de Nederlandse regering de Europese Commissie bij brief van 6 juli 2018 heeft meegedeeld dat Nederland enkele richtlijnbepalingen al heeft geïmplementeerd, namelijk de artikelen 5 (deels), 6, 7, 9 en 14 (deels). Artikel 7 (nationale strategie) is namelijk in april 2018 geïmplementeerd door de vaststelling van de Nederlandse cybersecurityagenda (NCSA),[3] en de overige genoemde bepalingen (aanwijzing CSIRT voor AED's en verplichting om ernstige ICT-incidenten te melden bij dat CSIRT) zijn voor de meeste aanbieders ten aanzien waarvan de Nederlandse regering voornemens is om ze aan te wijzen als AED, sinds 1 oktober 2017 respectievelijk 1 januari 2018 geïmplementeerd door middel van de Wgmc en het Besluit meldplicht cybersecurity (meldplicht voor aangewezen vitale aanbieders).
Daarnaast doet Nederland volwaardig mee in de door de NIB-richtlijn op EU-niveau gecreëerde gremia, te weten de samenwerkingsgroep en het CSIRT-netwerk (artikelen 11 en 12 NIB-richtlijn). De door de NIB-richtlijn beoogde minimumharmonisatie, alsook de samenwerking en afstemming op EU-niveau, zijn hiermee op gang gekomen.

De leden van de PvdA-fractie zien het voorliggende wetsvoorstel als een stap in de richting van het verbeteren van cybersecurity en vernemen graag van de regering welke additionele stappen zij mogen verwachten.

In de zojuist genoemde NCSA zijn zeven hoofdambities geformuleerd en is een groot aantal concrete maatregelen aangekondigd om cybersecurity in Nederland te versterken. Ingezet wordt onder meer op het uitbreiden en verder opbouwen van detectie- en responscapaciteiten, zodat daadkrachtig kan worden gereageerd op cyberdreigingen, vitale processen worden extra beschermd, er wordt flink geïnvesteerd in onderzoek en kennisontwikkeling en burgers en bedrijven worden door bewustwordingscampagnes meer en beter op de hoogte worden gebracht van digitale risico's. Bovendien wordt gewerkt aan een landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden. Publiek-private samenwerking is een belangrijk uitgangspunt van de NCSA. Jaarlijks zal over de voortgang van de maatregelen worden gerapporteerd in samenhang met het – eveneens jaarlijkse – Cyber Security Beeld Nederland, waarin de actuele dreigingen op cybersecurityterrein in kaart gebracht worden.

Ook vragen deze leden wat de inzet van Nederland is om cybersecurity verder op Europees niveau aan te pakken.

De Nederlandse inzet op cybersecuritygebied is vervat in de NCSA, en de bijbehorende Roadmap Digitaal Veilige Hard- en Software. Het grensoverschrijdende karakter van dreigingen maakt het noodzakelijk sterk in te zetten op internationale samenwerking. Een aantal doelstellingen van de

[2] http://europa.eu/rapid/press-release_MEMO-18-4486_nl.htm.
[3] Kamerstukken II 2017/18, 26 643, nr. 536.

NCSA kan slechts bereikt worden door middel van internationale wetgeving, coalitievorming of internationale ontwikkeling van normen en standaarden, in het bijzonder in Europees verband. Een concreet voorbeeld hiervan is de Nederlandse inzet in Brussel op snelle vaststelling van de Cyber Security Act en een voortvarende ontwikkeling van een Europees raamwerk Beveiligingscertificering voor ICT-producten en -diensten. Ook dringt het kabinet aan op het vaststellen van verplichte certificering voor specifieke productgroepen. Een ander voorbeeld is het nastreven van Europese samenwerking voor wat betreft het invullen van de behoefte aan goed opgeleid cybersecuritypersoneel, onder meer via onderwijs. Daarnaast blijft Nederland op onderwerpen als kwetsbaarheid van vrije software zijn rol als internetpionier vervullen.

Ten slotte constateren deze leden dat veel digitale dreigingen afkomstig zijn van statelijke actoren buiten Europa of van cybercriminelen die in landen buiten Europa actief zijn. Zij vragen welke ruimte de regering ziet en benut voor mondiale afspraken ter verbetering van cybersecurity.

Waar het gaat om de digitale dreiging van statelijke actoren buiten Europa spant de regering zich in voor de bestendiging van de toepassing van het bestaand internationaal recht in cyberspace en versterking van het normatief kader. Het internationaal recht, versterkt met normen voor verantwoordelijk gedrag door staten is de hoeksteen van de internationale rechtsorde, zowel online als offline. Daarom spant Nederland zich in voor hervatting van de discussie hierover in VN-verband. Omdat normontwikkeling niet alleen een statelijke aangelegenheid is, steunt Nederland ook belangrijke initiatieven zoals de Global Commission for the Stability of Cyberspace (GCSC). Doordat in de GCSC vertegenwoordigers van alle belangengroepen zitten, hebben de door hen vastgestelde normen vanzelfsprekend draagvlak daarbinnen.

Nederland heeft in 2016 het initiatief genomen om in EU-verband richtsnoeren te ontwikkelen voor het treffen van maatregelen binnen het gemeenschappelijke buitenlandse en veiligheidsbeleid. Deze richtsnoeren zijn eind 2017 vastgesteld. Met de aanname van raadsconclusies (16 april 2018) over kwaadwillende cyberactiviteiten heeft de EU dit instrumentarium voor het eerst ingezet en de eerste schreden gezet om te komen tot een collectieve EU-reactie. Ook gaat het erom dat Nederland zelf met een adequate en gepaste reactie kan komen. Daartoe is, in lijn met de Geïntegreerde Buitenlandse en Veiligheidsstrategie in juni 2018 een diplomatiek reactiekader bij cyberincidenten vastgesteld.

De Nederlandse regering acht het van groot belang dat landen gemeenschappelijk optreden tegen grensoverschrijdende computercriminaliteit. De Europese Commissie heeft op 17 april 2018 voorstellen gedaan om de mogelijkheden voor grensoverschrijdende toegang tot data binnen strafrechtelijke procedures te vergroten en daarbij de bestaande problemen terug te dringen. De voorstellen voorzien in de mogelijkheden voor justitiële autoriteiten om een vordering tot verstrekking (European Production Order/Europees Verstrekkingsbevel) of bewaring (European Preservation Order/Europees Bewaringsbevel) van elektronisch bewijsmateriaal, te richten tot ondernemingen die hun diensten aanbieden in de Europese Unie.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus