Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

33 694 Internationale Veiligheidsstrategie

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 60 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 november 2020

Op 5 juli 2019 heb ik u een brief gestuurd over de internationale rechtsorde in het digitale domein (Kamerstukken 33 694 en 26 643, nr. 47). Die brief gaf aanleiding tot het aanvaarden door uw Kamer van de gewijzigde motie van de leden Verhoeven en Koopmans (Kamerstuk 33 694, nr. 56) om te komen tot verdere internationale coördinatie van politieke attributie van cyberaanvallen, inclusief initiatieven gericht op internationale capaciteitsopbouw, die bijdragen aan benodigde expertise voor technische attributie. Doel van deze brief is om, mede namens de Ministers van Binnenlandse Zaken en Koninkrijksrelaties, Justitie en Veiligheid, Defensie, alsmede de Staatssecretaris van Economische Zaken en Klimaat, uw Kamer te informeren over de uitvoering van deze motie en de bereikte resultaten.

Deze resultaten zijn bepaald geen eindpunt. Door de snelheid van technologische, geopolitieke en maatschappelijke ontwikkelingen is het noodzakelijk constant te blijven investeren en initiatieven te nemen. Door zijn actieve rol bevindt Nederland zich in de voorhoede van internationale discussies op cyberbeleid, een positie die recht doet aan belang dat Nederland hecht aan dit domein. De noodzaak vervolgstappen te nemen om in te spelen op nieuwe ontwikkelingen komt aan het einde van deze brief aan de orde.

De context waarin de internationale rechtsorde in het digitale domein bestaat, is sindsdien substantieel veranderd. Als gevolg van de COVID-19-pandemie is de wereld afhankelijker dan ooit van digitale processen. Waar mogelijk heeft het openbare leven zich verplaatst naar het digitale domein. Datzelfde nemen we ook waar in de internationale verhoudingen, nu steeds meer diplomatieke contacten virtueel plaatsvinden. De drukte in cyberspace neemt toe, en daarmee de kwetsbaarheden van samenlevingen en individuen die zich daar bewegen. De beschikbaarheid, integriteit en de vertrouwelijkheid van digitale processen is niet vanzelfsprekend. En daarmee neemt de noodzaak om de internationale rechtsorde in het digitale domein – waaronder waarborging van de

kst-33694-60
ISSN 0921 - 7371
's-Gravenhage 2020

mensenrechten – te versterken toe. Deze context maakt dat de Nederlandse beleidsinzet aan actualiteitswaarde heeft gewonnen.

De eerdergenoemde brief noemde twee sporen waarlangs de beleidsinzet loopt: het bestendigen van de internationale rechtsorde in het digitale domein, en het formuleren van diplomatieke en politieke respons op inbreuken. Als derde spoor zou ik – in de lijn van de motie Verhoeven en Koopmans – de capaciteitsopbouw willen toevoegen. Deze sporen zijn op hun beurt weer een uitwerking van de Nederlandse Cybersecurity Agenda (Kamerstuk 26 643, nr. 536)[1] en maken deel uit van de brede inspanning van het kabinet om de cyberweerbaarheid en -slagkracht van Nederland te verhogen.

Het vertrekpunt van internationale coördinatie, en daarmee het eerste spoor van beleidsinzet, is de vraag naar de volkenrechtelijke verplichtingen en aansprakelijkheden van staten in het internationale verkeer, waaronder ook het digitale domein begrepen is. Internationaal recht vormt, tezamen met aanvullende gedragsnormen en vertrouwenwekkende maatregelen, het normatief kader in cyberspace. Om dit normatieve kader te bestendigen en de kosten van normoverschrijdend gedrag in het digitale domein te verhogen, is adequate respons noodzakelijk.

In dergelijke gevallen is het tweede spoor van beleidsinzet van belang, namelijk het formuleren en inzetten van diplomatiek-politieke maatregelen. Nederland en de EU beschikken over meerdere diplomatieke instrumenten in hun resp. *cyber diplomacy toolboxes*, die naar gelang de ernst van de situatie in te zetten zijn. De keus om over te gaan tot een bepaalde vorm van respons vergt integrale afweging en besluitvorming, in samenspraak met de betrokken departementen.

Het aanbod van capaciteitsopbouw als derde spoor is noodzakelijk om andere landen te helpen nationale structuren op te zetten die bijdragen aan de ontwikkeling van hun nationale cybersecuritystelsels, om ze te betrekken bij de internationale discussie over het bevorderen van cybersecurity binnen internationaal rechtelijke kaders en om ze te ondersteunen om in lijn daarmee hun eigen responskaders te ontwikkelen.

Op al deze sporen is in het afgelopen jaar vooruitgang geboekt, mede als gevolg van de manier waarop Nederland internationaal heeft gehandeld. Door middel van initiatieven als het cybersanctieregime in de EU, normatieve bescherming van de publieke kern van het internet en de versterking van het Global Forum on Cyber Expertise heeft Nederland heeft Nederland de internationale cyberagenda mede vorm gegeven.

1. Bestendigen van de internationale rechtsorde in het cyberdomein door internationaal overleg

Nederland en gelijkgezinde landen bepleiten universele erkenning van de toepasselijkheid van het internationaal recht in het digitale domein, waaronder het Handvest van de Verenigde Naties, het internationaal oorlogsrecht, mensenrechten en het staatsaansprakelijkheidsrecht. Daarnaast zet Nederland zich in voor de ontwikkeling van en steun voor vrijwillige, niet-bindende gedragsnormen in het cyberdomein.

De internationale discussies hierover spelen zich allereerst af in verschillende werkgroepen binnen de Verenigde Naties: onder de Eerste Commissie van de Algemene Vergadering van de VN (AVVN) functioneren

[1] M.n. ambitie 2 over Internationale vrede en veiligheid in het digitale domein, p. 23–24.

de *United Nations Group of Governmental Experts* (UNGGE) en de *Open Ended Working Group* (OEWG), parallelle processen die in het leven geroepen zijn op initiatief van de VS resp. Rusland. De vooruitzichten op een harmonieuze afronding van beide processen zijn ongewis, als gevolg van toenemende geopolitieke spanningen tussen de VS, Rusland en ook China.

Nederland draagt in beide werkgroepen uit dat het internationaal recht landen in staat stelt zich te verweren tegen cyberdreigingen. Daarom stelt Nederland zich te weer tegen de pogingen van Rusland, China en andere landen om toepassing van bestaand internationaal recht in cyberspace slechts in beperkte mate te erkennen. Door in te zetten op tijdrovende onderhandelingen over een nieuw verdrag, vergroten zij het risico op afkalving van rechtsbescherming. Bovendien wil Nederland betere handvatten om implementatie te bevorderen van de aanvullende gedragsnormen, die de UNGGE in 2015 heeft opgesteld en die de AVVN heeft verwelkomd. Niet in de laatste plaats vraagt Nederland aandacht voor dreigingen gericht tegen de publieke kern van het internet[2], dreigingen tegen het ongestoord en veilig verloop van verkiezingen, en dreigingen tegen vitale infrastructuur.

Voor de Nederlandse ideeën is steeds meer draagvlak, ook omdat zij geënt zijn op werk van de, onder meer door Nederland gesteunde, *Global Commission on the Stability of Cyberspace* (GCSC), een groep wereldwijd erkende deskundigen uit overheids-, politieke, private en *civil society* kring. De positieve weerklank is niet alleen te vinden onder gelijkgestemde landen: in toenemende mate is hij ook te horen onder de leden van de G-77, de grootste groepering van staten in de VN. Het is voor het verdere draagvlak in de VN van groot belang om deze groep duurzaam te engageren.

Parallel aan de twee processen in de Eerste Commissie is in de Derde Commissie van de AVVN op initiatief van Rusland in 2019 een onderhandelingsproces over een nieuw *cybercrime* verdrag gestart. De ontwerpverdragsteksten die Rusland daar heeft ingebracht, gaan uit van een autocratische visie op het internet, waarin burgerlijke vrijheden niet vooropstaan. Daarnaast bestaat het risico dat een nieuw verdrag het begrip cybercrime zo breed interpreteert, dat het autoritaire regimes handvatten biedt om hun onwelgevallige elementen in *cyberspace* doelgerichter internationaal op te sporen en vervolgen. Nederland en andere gelijkgezinden geven prioriteit aan het universaliseren van het *Cybercrime*-verdrag van de Raad van Europa (het Verdrag van Boedapest van 2001, dat Nederland in 2010 heeft geratificeerd), dat inmiddels ook door diverse landen buiten Europa is geratificeerd. Het Verdrag van Boedapest biedt sterkere mensenrechtelijke waarborgen bij de bestrijding van *cybercrime* dan de Russische voorstellen.

Daarbij is Rusland bovendien aan het voorsorteren op de uitkomsten van een ander intergouvernementeel proces, dat onder auspiciën van het *United Nations Office on Drugs and Crime* (UNODC) staat: in de eerste helft van 2021 zullen in dat raamwerk nl. conclusies en aanbevelingen komen van een *open-ended intergovernmental expert group*, in 2011 ingesteld om een samenhangende studie te doen naar cybercrime en de

[2] Onder de publieke kern van het internet vallen de centrale protocollen en infrastructuur die het fundament vormen voor een goed functionerend internet; het vertoont kenmerken van een internationaal publiek goed dat afzonderlijke soevereine en particuliere belangen overstijgt. Zie de kabinetsreactie op advies nr. 94 «De publieke kern van het internet: naar een buitenlands internetbeleid» van de Wetenschappelijke Raad voor het Regeringsbeleid, Kamerstuk 26 643, nr. 411.

respons daarop van lidstaten, de internationale gemeenschap en de private sector. Uit de inventariserende sessies van de afgelopen jaren is af te leiden dat deze werkgroep zeer verdeeld is over de noodzaak van een nieuw internationaal verdrag en de nadruk legt op de noodzaak om aan capaciteitsopbouw en overdracht van kennis en expertise te werken. Nederland en gelijkgezinde landen steunen deze lijn.

De waarborging van mensenrechten in het digitale domein vindt plaats in alle van de hierboven genoemde processen, maar krijgt bovendien vorm via de Nederlandse inbreng in de Mensenrechtenraad (MRR). Zo heeft Nederland bij de aanvang van zijn MRR-lidmaatschap in de periode 2020–2022 met Estland en Ghana een bijeenkomst georganiseerd over de versterking van de mensenrechtenbenadering in cybersecurity, in nauwe samenwerking met de *Freedom Online Coalition.*

Naast deze discussies vindt ook internationaal overleg plaats over de technische normen en standaarden waaronder het internet functioneert. In organisaties als de *International Telecommunications Union* (ITU) en de *United Nations Conference on Trade and Development* (UNCTAD) proberen meerdere landen, China voorop, internationale internetstandaarden tot norm te verheffen die het bestaande publiek-private model, de zgn. *multi-stakeholder governance* van het internet, ondergraven. Aldus dreigt een versplintering van het internet, met bijkomende negatieve gevolgen voor de openheid, vrijheid en veiligheid van het internet. Om deze tendens tegen te gaan werkt Nederland aan versterking van de coördinatie en samenwerking met gelijkgezinde landen.

2. Versterken van gezamenlijk optreden door assertieve diplomatieke respons

Het bovenstaande maakt duidelijk dat Nederland veel baat heeft bij de bouw van coalities van landen die een gedeelde cybervisie hebben en bereid zijn deze gezamenlijk te verdedigen. Nederland heeft daarom op 23 september 2019 met de VS en Australië het *Joint Statement on Advancing Responsible Behaviour in Cyberspace* in de AVVN gelanceerd. Binnen de EU is Nederland een drijvende kracht achter de *EU Cyber Diplomacy Toolbox* en de aanname van het EU-cybersanctieregime in mei 2019. En in februari 2019 nam de NAVO een «gids» *(NATO Guide)* voor inzet aan, om beter te reageren op het volledige spectrum aan kwaadwillende cyberactiviteiten.

Door het vormen van dit soort coalities staat Nederland sterker wanneer er aanleiding is om te reageren op cyberaanvallen van buitenlandse actoren. Dat was bijv. het geval bij de verstoorde cyberoperatie van Rusland tegen de OPCW in Den Haag in 2018 en de Russische cyberagressie tegen Georgië in 2019. In beide gevallen gaf de internationale gemeenschap een stevig signaal af tegen de cyberactiviteiten van Rusland door Rusland publiekelijk aan te wijzen als verantwoordelijke. Belangrijke vervolgstap in de ontwikkeling van een krachtige EU-bijdrage aan assertiever cyberbeleid waren de cybersancties van de EU tegen vier Russische GROe-officieren verantwoordelijk voor de OPCW-*hack*, een onderdeel van de GROe als organisatie achter o.a. de *NotPetya*-aanval in 2017, twee Chinese staatsonderdanen en een Chinese entiteit verantwoordelijk voor economische spionage, en een Noord-Koreaanse entiteit verantwoordelijk voor o.a. de *WannaCry*-aanval in hetzelfde jaar. Op 22 oktober volgden sancties tegen twee GROe-officieren en een GROe-entiteit die betrokken waren bij de cyberaanval op de Bondsdag in 2015.

Een krachtig antwoord op cyberaanvallen vergt zowel binnen als buiten de EU en de NAVO een grote inspanning van Nederland, met een brede groep van gelijkgestemden of op bilateraal niveau, zoals met Australië. Dit begint in Nederland zelf met nauwe samenwerking van betrokken departementen en diensten. In 2018 is het diplomatiek responskader voor cyberincidenten opgesteld onder coördinatie van het Ministerie van Buitenlandse Zaken. Dit biedt een platform voor de betrokken ministeries en diensten om een antwoord te formuleren op cyberincidenten en op de toenemende geopolitieke spanning in cyberspace, waar nodig.

De recente voorbeelden van internationale coördinatie van publieke toerekening en de *listings* van individuen en entiteiten in het kader van het EU-sanctieregime maken duidelijk dat samenwerking loont. Langs de lijnen van deze voorbeelden zal de komende tijd verder worden gewerkt. Het doel is steeds het ontmoedigen van cyberaanvallen en het doen veranderen van ongewenst gedrag, waarbij sancties en ander gemeenschappelijk proactief diplomatiek optreden een middel zijn. Een belangrijk onderdeel van dit diplomatieke optreden is de dialoog, ook met landen die een offensief cyberprogramma tegen Nederland uitvoeren, zoals Rusland en China. In die dialoog moet ook worden gezocht naar mogelijkheden om samen te werken op gebieden van gedeeld belang (zoals bestrijding van *cybercrime)*. Daarnaast gebruikt Nederland deze dialoog om – achter gesloten deuren – duidelijk te maken dat het bepaalde vormen van cybergedrag afkeurt. Het sanctie-instrument werkt dan als een onontbeerlijke stok achter de deur om onverantwoord gedrag te ontmoedigen.

3. Vormen van coalities door versterkte capaciteitsopbouw

De Nederlandse diplomatieke inzet heeft tot doel brede consensus te bereiken en richt zich nadrukkelijk op landen die traditioneel een minder uitgesproken profiel kunnen of willen aannemen in het internationale debat over cyber. Deze handreiking krijgt niet alleen vorm via demarches en andere vormen van diplomatiek contact. Nederland ondersteunt bovendien activiteiten die bijdragen aan de capaciteitsopbouw in derde landen, niet in de laatste plaats in landen die we in VN-verband nodig hebben (G-77 landen) voor een brede coalitie ter bevordering van verantwoordelijk gedrag in het cyberdomein. Dit gebeurt onder meer via:

a) het Global Forum on Cyber Expertise (GFCE), met secretariaat in Den Haag, dat met name midden- en lage inkomenslanden actief steunt met opbouw van hun cyberweerbaarheid en de bestrijding van cybercrime. Het GFCE is per 1 januari 2020 op afstand geplaatst van de Nederlandse overheid en voorzien van eigen rechtspersoonlijkheid (stichting GFCE).
b) Het Nederlandse trainingsprogramma ter ondersteuning van de opbouw van juridische capaciteit aangaande cyber en internationaal recht in Latijns-Amerika, Azië en Europa, via regionale partners zoals de OAS, de OVSE, Singapore en Australië).
c) In Zuidelijk Afrika, Zuidoost-Azië en het Midden-Oosten organiseren cyberdiplomaten op Nederlandse ambassades rondetafelconferenties onder de noemer *Promoting the International Dimensions in National Cybersecurity Strategies*. Die conferenties helpen bij het uitdragen van de aanbevelingen van andere initiatieven die Nederland ondersteunt, o.a. via de GCSC, RightsCon, GFCE en de *Freedom Online Coalition*.
d) Nederland ondersteunt initiatieven om het maatschappelijk middenveld in deze landen meer te betrekken bij het vrij, toegankelijk en veilig houden van het internet. Zo worden NGOs en mensenrechtenverdedigers in staat gesteld om hun eigen digitale werkomgeving veilig te houden. Nederland steunt hen bijv. ook met trainingen om internetvrijheid en restricties (ongeoorloofd gebruik van surveillance software, *internet shutdowns)* in kaart te brengen; de resultaten kunnen zij

presenteren bij de VN in Genève en New York, om zo een bijdrage te leveren aan de hierboven genoemde discussies. Bovendien maakt Nederland zich binnen de VN hard voor deelname van het maatschappelijk middenveld aan het internationale debat, waar mogelijk.

4. Anticiperen op nieuwe uitdagingen

Kenmerkend voor het cyberdomein is de grote dynamiek: technologische ontwikkelingen, zeker wanneer deze gepaard gaan met geopolitieke verschuivingen leiden tot nieuwe uitdagingen, zoals bijv. de uitrol van nieuwe netwerktechnologie duidelijk illustreert. Daar komt bij dat we verscherpingen meemaken van de discussies over het *governance model* van het internet en over burgerlijke vrijheden in *cyberspace.* Het internet als vector voor vrije en openbare meningsvorming en -uiting, en als een veilige ruimte voor vereniging staat onder druk van landen en partijen die dezelfde vrijheden in eigen land onderdrukken. En de context van de COVID-19-pandemie heeft niet geleid tot een toename van verantwoordelijk gedrag in het internationale verkeer. Het tegendeel is waar.

Nu is de discussie over het eigenaarschap van het internet zo oud als het internet zelf. En tot enkele jaren geleden was de verwachting reëel dat de steun toenam voor een model voor *internet governance* dat recht doet aan alle publieke en private belangen die bij het internet betrokken zijn. Helaas is de trend ten gunste van een versterkt *multi-stakeholder model* zoals Nederland dat voorstaat, tegenwoordig minder gunstig en is – als gezegd – de dreiging van de opkomst van een *splinternet* is reëel. Het is geen toeval dat westerse landen zich ook op dit vlak geplaatst zien tegenover Rusland en China, aangevuld met gelijkgezinde landen als Cuba, Iran, Nicaragua, Noord-Korea en Venezuela. Meerdere landen zijn bovendien actief om het digitale domein te gebruiken voor het verspreiden van desinformatie in andere landen.

Zo logenstraft de werkelijkheid het ideaal van een open, vrij en veilig internet steeds meer. De aanwezigheid van terroristische *online content*, van *online* desinformatie en van *hate speech* toont dat de regelloosheid en vrijheid, die ooit synoniem waren met het internet, ook zijn keerzijdes kent. Het spreekt voor zich dat de overheden een taak hebben om illegale *content* en inbreuken op de openbare orde tegen te gaan, *offline* én *online*. Daar waar het gaat om ongewenste, maar niet onrechtmatige *content*, waaronder een groot aantal verschijningsvormen van desinformatie onder valt, vraagt deze waardenspanning om zorgvuldige weging.

Zoals de Adviesraad Internationale Veiligheid (AIV) onlangs al duidelijk maakte in zijn advies over *online content*, zal Nederland zich in moeten zetten voor een open, vrij en veilig internet *binnen* de grenzen van democratische en rechtstatelijke waarden (waaronder in het bijzonder de bescherming van mensenrechten). Hoewel dit waarschijnlijk ingevuld zal worden door middel van wet- en regelgeving in Nederland en Europa, zullen de keuzes die hierin gemaakt worden, vanwege het grensoverschrijdende karakter van het internet, effect hebben op de werking van het internet wereldwijd. Een goed voorbeeld hiervan is de introductie van de Algemene Verordening Gegevensbescherming (AVG). Het kabinet zal uw Kamer nog nader informeren naar aanleiding van dit AIV-advies, over de mogelijkheden om deze rechten en vrijheden van een open internet te verzekeren en te bevorderen en tegelijkertijd schadelijke invloeden op het internet tegen te gaan. Hierbij moet in oog worden gehouden dat regelgeving over *online content* geen fragmentatie van het open en vrije wereldwijde internet mag veroorzaken, en recht moet doen aan de *end-to-end* interconnectie van de vele netwerken, die samen het internet vormen.

Door de potentiële destabiliserende werking van desinformatie is de aanpak van desinformatie van belang, waarbij het uitgangspunt is dat rechtsstatelijke waarden en grondrechten als de vrijheid van meningsuiting voorop staan. De Nederlandse houding ten opzichte van desinformatie gaat uit van de veerkracht van de samenleving en van ons pluriforme medialandschap, om de negatieve gevolgen van desinformatie tegen te gaan. Deze visie zal Nederland in de EU en wereldwijd blijven uitdragen. Via de *Freedom Online Coalition*, in 2011 geïnitieerd door Nederland en de VS, blijft ons land respect voor burgerlijke vrijheden in het digitale domein bevorderen. Binnen de *Freedom Online Coalition* zet Nederland zich in voor gezamenlijke verklaringen over onder meer kunstmatige intelligentie en desinformatie. Uitgangspunt is dat deze verklaringen een opmaat kunnen zijn naar breed gedeelde teksten, zoals VN-resoluties in New York of Genève.

Deze ontwikkelingen zijn gaande terwijl de onmisbaarheid van het internet voor het goed functioneren van onze economie en maatschappij steeds meer evident is. De COVID-19-pandemie heeft dit proces verder versneld. Daarbovenop komt de ontwikkeling van een nieuwe generatie mobiele netwerken: 5G zal naar verwachting een significante toename faciliteren van hard- en software die aan het internet is gekoppeld en die van grote invloed zal zijn op het maatschappelijk leven.

Gezien de internationale verhoudingen op het gebied van verdere technische ontwikkeling en de uitrol van 5G, bestaan er zorgen over risico's die samenhangen met toeleveranciers van deze technologie. Om de veiligheid en integriteit van deze netwerken te borgen zet Nederland – naast de nationale aanvullende beveiligingsmaatregelen (zie Kamerstuk 30 821, nr. 92 en Stb. 2019, nr. 457) in op een gezamenlijke Europese aanpak voor de veiligheid van 5G-netwerken (Kamerstuk 22 112, nr. 2816), conform de moties van de leden Weverling c.s. en Van den Berg c.s. (Kamerstuk 21 501-33, nrs. 734 en 747). Een Europese aanpak en uitwisseling van informatie over risico's en maatregelen zal bijdragen aan de effectiviteit van nationale en internationale beveiligingsmaatregelen.

5. 2021 en verder: vasthouden aan bestaande beleidskaders, verdere inspanning

Van de persoonlijke levenssfeer van burgers tot de veiligheid van vitale processen en van het verdienvermogen van bedrijven tot de werking van de overheid, de Nederlandse maatschappij is en blijft afhankelijk van het internet.

Tegen de achtergrond van de versnelling van de technologische revolutie en de snel verslechterende geopolitieke en -economische context blijven de drie sporen van de Nederlandse beleidsinzet in het internationale cyberdomein richtinggevend: het bestendigen van de internationale rechtsorde in het digitale domein, het formuleren van diplomatieke en politieke respons op inbreuken en het versterken van internationale samenwerking, ondersteund door capaciteitsopbouw, met als doel een open, vrij en veilig internet.

Om aan nieuwe uitdagingen het hoofd te bieden is verdere inspanning vereist. Nederland heeft zich – zoals hierboven geschetst – in de voorhoede geplaatst van de internationale discussies over het cyberbeleid. Om in een dynamische omgeving deze rol te blijven spelen zal het kabinet samen met nationale en internationale partners – in wisselwerking met en gebruikmakend van kennis en expertise in het bedrijfsleven,

wetenschap en maatschappelijk middenveld – bezien hoe de internationale rechtsorde, ook bij het gebruik van nieuwe technologieën, verder versterkt kan worden.

De Minister van Buitenlandse Zaken,
S.A. Blok