Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

33 694 Internationale Veiligheidsstrategie

Nr. 62

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 11 februari 2021

De vaste commissie voor Buitenlandse Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Buitenlandse Zaken over de brief van 16 november 2021 inzake de internationale rechtsorde in het digitale domein (Kamerbrief 33 694, nr. 60).

De vragen en opmerkingen zijn op 9 december 2020 aan de Minister van Buitenlandse Zaken voorgelegd. Bij brief van 9 februari 2021 zijn de vragen beantwoord.

De voorzitter van de commissie,
Pia Dijkstra

De adjunct-griffier van de commissie,
Konings

kst-33694-62
ISSN 0921 - 7371
's-Gravenhage 2021

I. Vragen en antwoorden

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de brief over de internationale rechtsorde in het digitale domein. Wel hebben deze leden nog een aantal vragen.
De leden van de VVD-fractie vinden het goed dat Nederland zich actief inzet voor de verbetering van de internationale rechtsorde in het digitaal domein. Zij vragen of ook andere landen het belang van dit thema voldoende inzien. Kunt u beschrijven wat Nederland doet om andere landen op het belang van dit thema te wijzen?
Het gaat daarbij voor deze leden niet alleen om het algemene begrip van de internationale rechtsorde, maar ook om specifieke internationale misdrijven, waaronder digitaal terrorisme, de potentieel ontwrichtende werking van *deepfakes* en de bijna per definitie grensoverschrijdende vergrijpen tegen de horizontale privacy, waaronder wraakporno en de alomvattende surveillance van personen. Wat is de inzet van Nederland voor de internationale bescherming van data omtrent individuen, nu door het verzamelen van momenteel internationaal verspreide data effectief het gehele leven van iemand in kaart kan worden gebracht, met alle gevolgen van dien voor de veiligheid en vrijheid van personen?

1. Antwoord van het kabinet

De inzet van het kabinet voor het versterken en handhaven van de rechtsorde op het internet geldt in de breedste zin van het woord, en komt aan de orde in een veelheid van overleggen met derde landen, zowel bilateraal als multilateraal. Niet alleen is er aandacht voor het tegengaan van illegale activiteiten, bijv. van terroristische content online of discriminatie online; ook het verankeren van fundamentele rechten in het online domein (zoals bijvoorbeeld het beschermen van privacy) via richtlijnen en regelgeving komt aan bod. Deze inzet toont Nederland in bilaterale diplomatieke contacten en bij overleggen in relevante internationale instellingen: EU, Raad van Europa, OVSE en VN. Vooral in de EU grijpt het kabinet de mogelijkheid aan om deze inzet te doen vertalen in wet- en regelgeving zoals dat bij persoonsgegevens is gebeurd in de Algemene Verordening Gegevensbescherming (AVG): die biedt in de EU het juridisch kader voor de bescherming daarvan. De omvang van de Europese markt maakt het aannemelijk dat ook niet-Europese internetbedrijven de Europese regelgeving zullen toepassen, bij voorkeur ook buiten de EU. De Europese Commissie heeft in december 2020 verschillende initiatieven op dit vlak gepresenteerd, zoals het *European Democracy Action Plan* en de *Digital Services Act*. Het kabinet is deze initiatieven momenteel aan het bestuderen en zal spoedig appreciaties hiervan naar uw Kamer versturen.

De leden van de VVD-fractie zijn verheugd te lezen dat Nederland, in de lijn met motie van de leden Verhoeven en Koopmans (Kamerstuk 33 694, nr. 56), werk maakt van capaciteitsopbouw. Wat doet Nederland om andere landen te helpen met capaciteitsopbouw en welke landen zijn dit? Wat gebeurt er op EU-niveau op het gebied van capaciteitsopbouw?

2. Antwoord van het kabinet

De steun die Nederland geeft aan capaciteitsopbouw is overwegend generiek van aard, en gericht op het scheppen en verder ontwikkelen van netwerken voor de uitwisseling van

cyber-gerelateerde kennis die aan meerdere landen tegelijkertijd ten goede komt. Het maakt daarbij gebruik van intermediaire instellingen zoals het GFCE, de Wereldbank en regionale organisaties als de OAS en de OVSE. In het kader van het GFCE wordt o.m. expertise uitgewisseld over het opstellen van nationale cybersecurity-strategieën en het oprichten van internetnooddiensten. In de ASEAN-regio werkt Nederland samen met Singapore en Australië dat met Nederlandse steun cursussen aanbiedt aan landen in de regio. In Latijns-Amerika biedt Nederland dergelijke cursussen aan in samenwerking met de OAS. Ook met de OVSE zijn dergelijke programma's opgezet. In 2020 heeft Nederland ook een project in Servië ondersteund ten behoeve van de versteviging van publiek-private samenwerking op cybersecurity-gebied. Daarnaast steunt Nederland capaciteitsopbouw via de *Freedom Online Coalition* (FOC) en aan NGO's, dat laatste in Argentinië, Chili, Ecuador, Mexico, Panama, Peru, Ghana, Kenya, Nigeria, Liberia, Indonesië en Maleisië.
De EU is een belangrijke kennisbron voor cybercapaciteitsopbouw via instellingen als ENISA, Eurojust en Europol, en treedt op als financier en als uitvoerder van een twintigtal activiteiten op dat terrein. De hoofdlijnen van de strategie van de EU voor cybercapaciteitsopbouw is thans neergelegd in de EU Externe Cyber Capaciteitsopbouw Richtsnoeren[1]. De focus van de EU is primair op de Westelijke Balkan en de nabuurschapslanden gericht. Nederland draagt bij aan het Cyber4Dev programma dat zich richt op landen in Afrika en Azië.
Op 16 december 2020 hebben de Commissie en Hoge Vertegenwoordiger (HV) uiteengezet welke toekomstige ambities de EU zou moeten nastreven op het gebied van *cyber security*. In een gemeenschappelijke verklaring aan de Raad en het EP *The EU's Cybersecurity Strategy for the Digital Decade* gaan zij daarbij ook in op capaciteitsopbouw: de geografische focus zou ongewijzigd moeten blijven, en cybersecurity moet voortaan een standaard element zijn in projecten met een digitaliseringscomponent. De EU moet deze landen ook helpen bij het aanpakken van de kwaadwillige cyberactiviteiten die de integriteit en veiligheid van democratische systemen schaden. *Peer-to-peer learning* tussen EU-lidstaten en relevante EU-agentschappen en derde landen zou in dit opzicht nuttig zijn, aldus Commissie en HV, die ook de instelling van een *EU Cyber Capacity Building Board* bepleiten, om samenwerking en synergie te bevorderen tussen de verschillende institutionele belanghebbenden in de EU. Het kabinet is zal spoedig een appreciatie van deze EU Cybersecurity Strategie naar uw Kamer versturen.

De VVD-fractieleden vragen welke «gelijkgezinde» landen universele erkenning van de toepasselijkheid van het internationaal recht in het digitale domein bepleiten. Door welke landen wordt Nederland hierin gesteund? Welke stappen zijn er al gezet en wat is er al bereikt op het gebied van vrijwillige, niet-bindende gedragsnormen in het cyberdomein?

3. Antwoord van het kabinet

Reeds in 2013 is in het consensus rapport van de toenmalige *United Nations Group of Governmental Experts* (UNGGE) onder de Eerste Commissie van de Algemene Vergadering van de VN (AVVN) o.a. overeengekomen dat internationaal recht van toepassing is in het digitale domein. In 2015 werd hierop

[1] https://data.consilium.europa.eu/doc/document/ST-10496–2018-INIT/en/pdf.

voortgebouwd door het benoemen van specifieke beginselen zoals het verbod op interventie in de interne aangelegenheden van een andere staat. Op het gebied van vrijwillige, niet-bindende gedragsnormen in het cyberdomein zijn er elf normen overeengekomen in het consensus rapport van de UNGGE in 2015. Deze normen zijn door de AVVN unaniem verwelkomd. In de huidige onderhandelingen van de GGE 2019–2021 bespreekt men een *additional layer of understanding* ter verdere implementatie en operationalisering van o.m. deze elf normen. Nederland vraagt daarbij specifiek aandacht voor dreigingen gericht tegen de publieke kern van het internet, dreigingen tegen het ongestoord en veilig verloop van verkiezingen, en dreigingen tegen vitale infrastructuur.

Alle leden van de VN hebben dus in principe de erkenning van de toepasbaarheid van internationaal recht in het digitale domein erkend. Een coalitie van landen onder aanvoering van China en Rusland poogt hier afbreuk aan te doen door te beargumenteren dat in aanvulling op bestaande regels een nieuw verdrag nodig is. Het onderhandelen van een nieuw verdrag kan jaren of decennia duren, zeker wanneer hiervoor geen momentum bestaat, dan wel op brede steun van het VN lidmaatschap kan worden gerekend. Hierdoor ontstaan er verschillende kampen binnen de VN. Aan de ene kant zijn er landen die op het internationaal recht georiënteerd zijn, waaronder Nederland. Landen in de GGE die (grotendeels) op de Nederlandse lijn zitten zijn Australië, Brazilië, Duitsland, Estland, Frankrijk, Mexico, Noorwegen, Japan, Uruguay, Roemenië, de Verenigde Staten, het Verenigd Koninkrijk en Zwitserland. Aan de andere kant staan de meer staatsgeoriënteerde landen die pleiten voor meer controle van staten en mitsdien een beperkte toepasbaarheid van internationaal recht. Tussen deze uitersten van het spectrum bevindt zich een grote groep landen die nog geen duidelijk keuze heeft gemaakt, de *swing states*. Nederland wil landen in deze groep ervan overtuigen dat zij op basis van hun nationale politiek-economische en sociaal-maatschappelijke belangen juist baat hebben bij een vrij, open en veilig internet. Een voorbeeld van het optrekken met gelijkgezinde landen is het *Joint Statement on Advancing Responsible Behaviour in Cyberspace* dat Nederland gezamenlijk met 26 andere staten, waaronder de V.S., tijdens AVVN in 2019 heeft gelanceerd.

Deze leden vragen tegelijkertijd aandacht voor de wenselijkheid van regulering daar waar dit effectief en mogelijk zou zijn, teneinde de veiligheid en vrijheid van mensen beter te beschermen. Welke mogelijkheden ziet het kabinet hiertoe? Wanneer en onder welke omstandigheden ziet het kabinet ruimte om gezamenlijke initiatieven te ondernemen voor concrete normering? Ziet het kabinet ruimte om eventueel in een beperktere kring van democratische gezinde landen over te gaan tot verdere normering en collectieve afspraken?

4. Antwoord van het kabinet

Op het gebied van de regulering van online content bereidt het kabinet momenteel een reactie op het eerder verschenen advies van de Adviesraad Internationale Vraagstukken *«Regulering van Online Content, Naar een herijking van het Nederlandse internetbeleid»*. Deze reactie zal in de eerste maanden van 2021 naar de kamer gestuurd worden.

De leden van de VVD-fractie zijn verheugd te zien dat Nederland zich actief uitspreekt tegen cybercrime op internetplatforms. Hoe succesvol is de dialoog over samenwerking op dit gebied tot dusver? Hoe ziet de Nederlandse regering de rol van online sociale platforms maar ook van darkweb/illegale platforms? Op welke wijze werkt Nederland samen met Facebook en andere legale platforms om vormen van terroristische online content tegen te gaan?

5. Antwoord van het kabinet

Het tegengaan van cybercrime en online illegale activiteiten blijft een speerpunt in het Nederlands internetbeleid. Een goede samenwerking met de internetplatforms op dit vlak blijft dan ook noodzakelijk, en hetzelfde geldt voor het tegengaan van terroristische *online content*. Daartoe heeft Nederland in 2019 de *Christchurch call* ondertekend, waarin 48 landen en acht bedrijven (o.a. Facebook, Google, Microsoft, Twitter en YouTube) zich verplichten om een einde te maken aan (de promotie van) online terrorisme en gewelddadig extremisme. Deze oproep leidde onder meer tot de oprichting van de GIFCT *(Global Internet Forum to Counter Terrorism)*, waarin bedrijven samenwerken om online terroristische content tegen te gaan en snel te verwijderen. De Europese Commissie heeft deze aspecten ook meegenomen in de *Digital Services Act*, zoals in december 2020 gepresenteerd.

Voorts is op 10 december 2020 een politiek akkoord gesloten over de *EU-verordening voor het tegengaan van de verspreiding van terroristische online content*. Naar verwachting wordt de verordening begin april 2021 gepubliceerd en is er een 12 maanden implementatietermijn. De verordening beoogt onder andere een (grensoverschrijdend) systeem waarmee terroristische uitlatingen zo snel mogelijk van internet worden gehaald. De verordening vereist ook dat iedere lidstaat een of meerdere competente autoriteit(en) opricht of aanwijst. Deze autoriteit krijgt in Nederland de vorm van een Zelfstandig Bestuursorgaan die zich gaat bezighouden met twee taken: de bestrijding van online kinderpornografisch materiaal én de bestrijding van online terroristisch materiaal[2].

De leden van de VVD-fractie pleiten er bovendien voor dat Europese landen meer samen optrekken bij het aanpakken van de daders achter cyberaanvallen, zeker waar dit statelijke actoren betreft. Het EU-sanctieregime is dan ook een goede eerste stap, maar niet voldoende. Bij een hack die zware fysieke schade veroorzaakt, geldt in principe het recht op collectieve zelfverdediging, maar bij de meeste van de huidige cyberaanvallen geldt er beweerdelijk geen recht op collectieve tegenmaatregelen. Landen mogen dit allen zelf doen. Dat maakt kleinere landen binnen de NAVO of de Europese Unie een aantrekkelijker prooi voor kwaadwillende landen, en is dus niet in het belang van onze veiligheid. Deelt het kabinet de mening dat we moeten kijken naar manieren om hier samen op te trekken?

[2] zie Kamerbrief Autoriteit kinderpornografisch materiaal en terroristische content, Kamerstuk 31 015, nr. 208.

6. Antwoord van het kabinet

Een staat die het doelwit is van een cyberoperatie, die gekwalificeerd kan worden als een gewapende aanval, mag in bepaalde omstandigheden gebruik maken van het inherente recht tot (collectieve) zelfverdediging en geweld gebruiken om zichzelf te verdedigen. Dit recht is neergelegd in artikel 51 van het VN-Handvest. De getroffen staat mag hierbij hulp vragen aan andere staten. Waar het recht op collectieve zelfverdediging tegen een gewapende aanval een gevestigd begrip is in het internationaal recht, geldt dat niet voor het nemen van collectieve tegenmaatregelen *(countermeasures)* tegen een schending van een internationaalrechtelijke verplichting die geen gewapende aanval zijn.

Een staat mag onder bepaalde voorwaarden tegenmaatregelen nemen tegen een schending van een internationaalrechtelijke verplichting door een andere staat waarvan hij slachtoffer is (internationaal onrechtmatige daad). De tegenmaatregel zou normaliter een schending opleveren van een internationaalrechtelijke verplichting, maar is geoorloofd wanneer het een reactie is op een eerdere schending door een andere staat. Het nemen van tegenmaatregelen is gebonden aan strikte eisen. De tegenmaatregel mag bijvoorbeeld niet de drempel van geweldgebruik (zoals bij een gewapende aanval wel mogelijk zou kunnen zijn) bereiken.

Anders dan bij het recht op zelfverdediging, mag de getroffen staat geen beroep doen op andere staten (waaronder bondgenoten) om de maatregel collectief uit te voeren. De assisterende staat zou dan namelijk zelf het internationaal recht schenden, want alleen de slachtofferstaat is geoorloofd te reageren met een handeling die normaliter een onrechtmatige daad zou opleveren. Op dit moment is er geen regel van internationaal recht die het nemen van collectieve tegenmaatregelen mogelijk maakt.

Wel bestaan er mogelijkheden voor het ondersteunen van andere staten wanneer deze tegenmaatregelen uitvoeren. Die steun kan echter slechts bestaan uit handelingen die geen schending van internationaal recht opleveren. Verder heeft de NAVO tijdens de Defensie Ministeriele Conferentie in 2019 de zogenaamde *Guide for Strategic Response Options to Malicious Cyber Activity* aangenomen. Daarin wordt een overzicht geschetst van responsopties voor NAVO op schadelijke cyberaanvallen die het routinematige ontstijgen, maar waarvan het effect niet dusdanig schadelijk dat er sprake kan zijn van een gewapende aanval (en inroepen van artikel 5) of het nemen van collectieve tegenmaatregelen.

Behalve tegenmaatregelen en collectieve zelfverdediging bestaan er nog andere opties om te reageren op gedragingen van een andere staat in het cyberdomein. Deze heeft het kabinet eerder uiteengezet in de bijlage van de Kamerbrief uit 2019 (Kamerstuk 33 694 nr. 47), maar in het licht van deze beantwoording is het waardevol deze nogmaals te herhalen. *Retorsie* is impliciet al behandeld en is ook hetgeen waar het cybersanctieregime zich op baseert. *Noodzaak* is een rechtvaardigingsgrond die onder bepaalde strikte voorwaarden rechtvaardiging biedt voor handelen dat anders als internationaal onrechtmatig zou worden bestempeld, zoals bijvoorbeeld het inzetten van offensieve

cybermiddelen tegen een andere staat. De mogelijkheden van het principe van *noodzaak* worden op dit moment door dit kabinet verder verkend mede in het licht van mogelijke veiligheidspolitieke gevolgen.

Het kabinet is van mening dat cyberaanvallen idealiter in coalitieverband moeten worden geadresseerd. Nederland onderstreept daarom het belang van samenwerking met o.a. NAVO-bondgenoten en EU-lidstaten in het aanpakken van cyberaanvallers. De actieve bijdrage van Nederland aan het EU-cybersanctieregime is hiervan een concreet voorbeeld. Overigens geldt het belang van coalitievorming ook buiten de EU- en NAVO-kaders, zo heeft Nederland in een coalitie van gelijkgezinde landen de Russische cyber-aanvallen op Georgië veroordeeld.

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben met interesse kennisgenomen van de brief over de internationale rechtsorde in het digitale domein en zijn verheugd dat het kabinet aan de slag is gegaan met de 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. Deze leden hebben nog enkele vragen.

De leden van de D66-fractie lezen dat Rusland inzet op een verdrag naar cybercrime zonder voldoende waarborgen voor (digitale) burgerlijke vrijheden. Kan het kabinet toelichten welke mensenrechtelijke waarborgen het Verdrag van Boedapest biedt in vergelijking met de Russische voorstellen?

7. Antwoord van het kabinet

De Cybercrime Conventie van de Raad van Europa (Boedapest Conventie) biedt in de preambule en in artikel 15 specifieke waarborgen voor burgerlijke vrijheden, zoals de noodzaak om een juiste balans te vinden tussen de belangen van rechtshandhaving en respect voor fundamentele mensenrechten, het expliciet benoemen van de vrijheid van meningsuiting, het recht om informatie en ideeën te verspreiden en het recht op privacy en gegevensbescherming. Bovendien is er in artikel 15 sprake van dat staten verplicht zijn om de bepalingen van de Conventie uit te voeren op een wijze die in overeenstemming is met hun internationaalrechtelijke verplichtingen onder internationale mensenrechtenverdragen en het principe van proportionaliteit te waarborgen. Het meest recente Russische voorstel[3] verwijst enkel in algemene bewoordingen in de preambule naar «universeel erkende principes en normen van internationaal recht». Daarnaast wordt het principe van proportionaliteit niet genoemd in deze Russische concept-conventie. In de huidige onderhandelingen over een Tweede Aanvullend Protocol bij de Boedapest Conventie maken Nederland en de EU zich sterk voor waarborgen met betrekking tot privacy en data-bescherming die in overeenstemming zijn met de AVG.

[3] https://www.rusemb.org.uk/fnapr/6394.

De leden van de D66-fractie horen graag dat Nederland zich sterk inzet tegen kwaadwillende cyberactiviteiten en dat Nederland coalities vormt wanneer er aanleiding is om te reageren op cyberaanvallen van buitenlandse actoren. Het kabinet schrijft: «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.» Om welke gelijkgestemde landen gaat het hier? Hoe vaak is er gebruik gemaakt van publieke toerekening en de *listings* van individuen en entiteiten in het kader van het EU-sanctieregime?

8. Antwoord van het kabinet

Nederland werkt samen met landen die een vergelijkbare visie hebben op regels en normen in het cyberdomein. Met welke landen wordt samengewerkt in specifieke gevallen hangt af van de context waarin een cyberaanval plaatsvindt. Zo ligt het voor de hand om samen te werken met andere landen die ook slachtoffer zijn van de aanval. Daarnaast is van belang of landen bereid zijn cyberaanvallen publiek toe te rekenen.

In juli 2020 zijn er EU-sancties aangenomen tegen zes personen en drie entiteiten afkomstig uit drie landen, n.a.v. verschillende cyberaanvallen, waaronder tegen de OPCW. Op 22 oktober volgden sancties tegen twee GROe-officieren en een GROe-entiteit die betrokken waren bij de cyberaanval op de Bondsdag in 2015. Het sanctieregime is uitdrukkelijk gericht op personen en entiteiten. Het listen van deze personen en entiteiten betreft nadrukkelijk geen publieke toerekening aan landen.

Vragen en opmerkingen van de leden van de GroenLinks-fractie

De leden van de GroenLinks-fractie hebben met interesse kennisgenomen van de kabinetsbrief over de internationale rechtsorde in het internationale domein. Gezien het snel toenemende belang van het digitale domein in de geopolitiek juichen zij de actieve rol die Nederland op zich heeft genomen met betrekking tot internationale discussies over cyberbeleid toe. Zij hebben daar nog enige vragen bij.

De leden van de GroenLinks-fractie lezen dat Nederland zich inzet voor de ontwikkeling van vrijwillige, niet-bindende gedragsnormen in het cyberdomein, maar dat de vooruitzichten ongewis zijn als gevolg van toenemende geopolitieke spanningen tussen de Verenigde Staten, Rusland en China. Dat baart deze leden zorgen. Op welke wijze zet het kabinet zich in om toch vooruitgang te kunnen boeken in deze uitdagende context? Is het de strategie om eerst met kleinere gelijkgezinde landen tot een gedragscode te komen? Of juist om geen stappen te zetten zolang de geopolitieke grootmachten niet meedoen? Kan het kabinet een voorbeeld geven van de betere handvatten die het kabinet voor ogen heeft om de implementatie van aanvullende gedragsnormen te bevorderen? En hoe verhouden de inspanningen van Nederland op dit terrein zich tot de ontwikkeling en inzet van offensieve cyber door Nederland zelf?

9. Antwoord van het kabinet

Het kabinet zet zich met gelijkgezinde landen binnen en buiten de VN in om het internationaal normatief kader ter regulering van cyberoperaties te bestendigen. Een voorbeeld van het optrekken met gelijkgezinde landen is *Joint Statement on Advancing Responsible Behaviour in Cyberspace* dat Nederland gezamenlijk

met 26 andere staten, waaronder de VS, tijdens AVVN in 2019 heeft gelanceerd. Het kabinet streeft geen aparte gedragscode na maar wil het draagvlak voor de erkenning van het bestaande normatieve kader bestendigen door coalities aan te gaan met landen.

In de eerdergenoemde werkgroepen binnen de Eerste Commissie van VN zet Nederland zich in voor de implementatie en daardoor operationalisering van de consensus-afspraken. Een concreet voorbeeld is de inzet van Nederland ter bescherming van de beschikbaarheid en integriteit van het internet.

Het kabinet is van mening dat de ontwikkeling en mogelijke inzet van militaire cybercapaciteiten legitiem en noodzakelijk is. Hiervan gaat bovendien een afschrikwekkende werking uit, wat invloed heeft op de afweging van een potentiële opponent om zich al dan niet aan internationale afspraken te houden. Uitgangspunt is wel dat de mogelijk inzet geschiedt volgens de kaders van het bestaand internationaal recht. Zoals reeds beschreven in de Internationale Cyberstrategie en de Defensie Cyberstrategie, is het kabinet transparant over de Nederlandse ambitie om militaire cybercapaciteiten te ontwikkelen. Op dat gebied pleit Nederland internationaal ook voor meer transparantie van andere landen. Transparantie op dit vlak is een vertrouwenwekkende maatregel die kan helpen om misverstanden te voorkomen, stabiliteit te vergroten en wantrouwen te verminderen. Dit kan een bijdrage leveren aan het bevorderen van de internationale rechtsorde in het digitale domein, het voorkomen van het ontstaan van een wapenwedloop en het wegnemen van wantrouwen en gevaar op escalatie en miscalculatie.

De leden van de GroenLinks-fractie delen de zorgen van het kabinet over de pogingen van China, en andere autocratische landen, om het *multi-stakeholder governance* model van het internet te ondergraven. Wel vragen zij zich af wat nu de beste strategie is om dit tegen te gaan. Op welke manier biedt Nederland actief tegenwicht aan China in discussies binnen de *International Telecommunications Union* (ITU), bijvoorbeeld door te bepleiten dat cruciale elementen van het *multi-stakeholder model*, zoals een stevige rol voor het maatschappelijk middenveld en brede aandacht voor mensenrechten in de digitale wereld, ook in ITU-verband worden verankerd? Ook zijn deze leden benieuwd welke rol het kabinet ziet weggelegd voor het *Internet Governance Forum* (IGF).

10. Antwoord van het kabinet

Al jaren is Nederland met veel andere landen voorstander van een open, veilig en vrij internet. Het internet wordt door een veelheid aan (non-profit) organisaties in stand gehouden, waardoor niet een enkele partij of overheid het internet beheert. Dit *multistakeholder model* is van groot belang voor Nederland en is recentelijk opnieuw bevestigd door de EU in de nieuwe EU cyber security strategie.
Nederland trekt op met EU lidstaten en gelijkgezinde landen om tegenwicht te bieden aan Chinese voorstellen die het *multistakeholder governance model* ondergraven. In VN-context onder de Eerste Commissie van de AVVN zijn meerdere consultaties met het maatschappelijk middenveld gehouden als onderdeel van de *Open-Ended Working Group* (OEWG) en *Governmental Group of Experts* (GGE). Binnen de FOC wordt samen met de private sector

en maatschappelijk middenveld opgetrokken om mensenrechten te waarborgen binnen VN discussies.

Nederland neemt actief deel aan ITU conferenties en studiegroepen. Tijdens de conferenties wordt de rol, het mandaat en werkmethoden van de ITU vormgegeven en in de studiegroepen worden wereldwijde standaarden op met name telecommunicatiegebied ontwikkeld. Nederland en andere EU lidstaten werken met betrekking tot ITU nauw samen met gelijkgezinde landen om mogelijkheden te zoeken het *multi-stakeholder model* in ITU op te nemen; tevens hebben de samenwerkende landen specifiek aandacht voor Chinese voorstellen die het open en vrije karakter van het internet in gevaar brengen.

Daarnaast onderschrijft het kabinet het belang van de open discussies volgens het *multi-stakeholder principe* binnen het *Internet Governance Forum* (IGF) en verleent het financiële steun aan de IGF. Het IGF is een open en inclusief platform, met een VN mandaat voor het initiëren en faciliteren van een wereldwijd debat over de ontwikkeling van het internet en de huidige en opkomende fenomenen die verband houden met het functioneren ervan. In de VN *Roadmap for Digital Cooperation* zijn aanbevelingen gedaan om de IGF-uitkomsten beter te verankeren. De eerste stappen zijn dit jaar gezet door stevigere toezeggingen van de sprekers, en de bedrijven of organisaties die zij vertegenwoordigen. In 2025 vindt het WSIS+20 *review* plaats waar Nederland de *multi-stakeholder* benadering op *internet governance* blijft nastreven.

De leden van de GroenLinks-fractie vragen of het kabinet wil aangeven op welke wijze Nederland werk maakt van de aanbeveling uit het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) over de publieke kern van het internet om de internetdiplomatie te verbreden, door zogenaamde *swing states* in Azië, Afrika en Latijns Amerika, te overtuigen om zich in te zetten voor het open, vrije internet.

11. Antwoord van het kabinet

Nederland heeft in 2020 virtuele Regionale Cyberdialogen in Zuidoost-Azië en Zuidelijk Afrika georganiseerd om regionale discussies te stimuleren tussen overheden, private sector, maatschappelijk middenveld en academische wereld over i) een open, veilig en vrij internet, ii) de bestendiging van de internationale rechtsorde door de toepassing van internationaal recht, iii) normen voor verantwoord gedrag in het digitale domein (o.a. de norm ter bescherming van de publieke kern van het internet), vertrouwenwekkende maatregelen tussen staten en benodigde capaciteitsopbouw. In 2021 zullen virtuele en fysieke Regionale Cyberdialogen volgen in Azië, Afrika en Latijns Amerika. Daarnaast draagt Nederland het streven naar een open, vrij en veilig Internet uit in globale fora, zoals ICANN, WSIS, OECD, ITU en IGF, waar dit aspect in aldaar gevoerde discussies die raken aan het *multi-stakeholder model of Internet Governance* aan de orde komt of ter discussie gesteld wordt. Door deze inzet levert Nederland een bijdrage aan de bevordering van een open, veilig en vrij internet.

De leden van de GroenLinks-fractie vragen op welke wijze Nederland zich binnen andere VN-organisaties inzet voor het vrije en open internet. Is het kabinet bereid om de adoptie van een resolutie over de vrijheid van het

internet te promoten bij de VN Mensenrechtenraad 2021, alsook een vervolgresolutie over nieuwe technologie en mensenrechten? En is het kabinet bereid om de *UN Roadmap for Digital Cooperation* te bevorderen en te zorgen dat het maatschappelijk middenveld hierbij wordt betrokken?

12. Antwoord van het kabinet

Op beide genoemde resoluties, maar ook andere resoluties met een mensenrechten online component (vrijheid van meningsuiting, ruimte voor maatschappelijk middenveld, mensenrechten en het internet) houdt het kabinet de ontwikkelingen nauwlettend in de gaten en blijft het zich inzetten voor een sterke resoluties op dit onderwerp. Hierin treedt Nederland vaak op in EU verband, maar ook middels de FOC.

Het doorlopende werk op de implementatie van de *UN Roadmap for Digital Cooperation* is niet gelimiteerd tot de deelname van staten. Het maatschappelijk middenveld neemt hier ook aan deel. Sterker nog, een ambitieuze agenda zoals de *roadmap* zou niet zonder het maatschappelijk middenveld bereikt kunnen worden. De implementatie ervan behoeft initiatieven vanuit de VN zelf en daarbuiten. Het kabinet onderschrijft daarbij de belangrijke rol van de onlangs benoemde *UN Tech Envoy* om de inclusiviteit en samenwerking met het maatschappelijk middenveld te waarborgen.

De leden van de GroenLinks-fractie delen de zorg van het kabinet dat de regelloosheid van het internet ook zijn keerzijde kent en dat landen overal ter wereld te maken krijgen met problematiek rond online desinformatie en *hate speech*. Dit speelt bijvoorbeeld een rol in het huidige conflict in Ethiopië, waar de grote internationale sociale mediabedrijven amper verantwoordelijkheid nemen en niet in de benodigde capaciteit hebben geïnvesteerd om content in de lokale talen te kunnen screenen, met mogelijk ontwrichtende gevolgen. Tegelijkertijd laat een recent rapport van *Amnesty International* zien dat *Facebook* en *Google* in Vietnam juist nauwelijks tegenwicht bieden aan verzoeken vanuit de Vietnamese autoriteiten om kritische geluiden te censureren. Hoe kijkt het kabinet naar de rol van internationale sociale mediabedrijven? Op welke wijze, en in welke internationale fora, kunnen die bedrijven worden gewezen op hun verantwoordelijkheden en daaraan worden gehouden?

13. Antwoord van het kabinet

Sociale mediabedrijven spelen een belangrijke rol in het tegengaan van illegale content en de verspreiding van desinformatie. Het kabinet onderschrijft dat de balans tussen niet ingrijpen – waarmee illegale content zoals *hatespeech* online blijft staan – en te sterk ingrijpen – waarmee mensen onrechtmatig beperkt in hun vrijheid van meningsuiting kunnen worden – in veel landen en gevallen nog gevonden moet worden. De grondrechten van burgers moeten gewaarborgd zijn.

Het kabinet is van mening dat internetbedrijven de definitie van vrijheid van meningsuiting, zoals opgenomen in de gebruiksvoorwaarden van hun platformen, zouden moeten baseren op internationale mensenrechtenstandaarden. Ook zouden deze bedrijven de *UN Guiding Principles on Business and Human Rights* moeten onderschrijven. Het kabinet draagt dit standpunt uit in zowel bilaterale gesprekken met deze bedrijven, maar ook op bijvoorbeeld het *Internet Governance Forum.*

Vragen en opmerkingen van de leden van de PvdA-fractie

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van de inzet van het kabinet op het gebied van internationale rechtsorde in het digitale domein. Het kabinet stelt terecht dat als gevolg van de COVID-19-pandemie de wereld afhankelijker dan ooit is van digitale processen, het openbare leven zich meer dan voorheen heeft verplaatst naar het digitale domein en dat daarmee de noodzaak om de internationale rechtsorde in het digitale domein – waaronder waarborging van de mensenrechten – te versterken, toeneemt. De leden van de PvdA-fractie hebben nog enkele vragen over deze brief.

De leden van de PvdA-fractie waarderen de inzet van Nederland om met gelijkgezinde landen te pleiten voor 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.

Nederland draagt in beide werkgroepen binnen de VN, de *United Nations Group of Governmental Experts* (UNGGE) en de *Open Ended Working Group* (OEWG), uit dat het internationaal recht landen in staat stelt zich te verweren tegen cyberdreigingen en niet in de laatste plaats vraagt Nederland aandacht voor dreigingen gericht tegen de publieke kern van het internet, dreigingen tegen het ongestoord en veilig verloop van verkiezingen, en dreigingen tegen vitale infrastructuur. De leden van de PvdA-fractie merken op dat dreigingen er ook uit bestaan dat bovenop de bestaande restricties van bepaalde regimes die de internetvrijheid beperken, er in reactie op de COVID-19-pandemie een veelheid aan maatregelen en wetgeving wereldwijd is ingevoerd waarvan het merendeel betrekking heeft op het censureren van online informatie of verregaande surveillance.[4] Hoe oordeelt het kabinet over de dreiging die uitgaat van de inzet van deze maatregelen en wetgeving die onder de noemer van volksgezondheid leidt tot vergaande inbreuken op mensenrechten waaronder privacy-schendingen?

14. Antwoord van het kabinet

Het kabinet is bezorgd over de verstrekkende wet- en regelgeving die door verschillende landen is ingevoerd en betrekking hebben op het censureren van online informatie of vergaande surveillance. Om deze reden onderschreef Nederland de gezamenlijke verklaring van de Freedom Online Coalition (FOC) van mei 2020 over COVID-19 en internetvrijheid[5]. In deze verklaring uitte de FOC haar bezorgdheid over de gevolgen van de bovengenoemde wet- en regelgeving die ingevoerd is naar aanleiding van de COVID-19-crisis, die bijv. leiden tot het gebruik van willekeurige of onwettige surveillance, internet *shutdowns* en censuur. De FOC roept regeringen over de hele wereld op om af te zien van het aannemen of implementeren van dergelijke wet- en regelgeving, die kunnen leiden tot een vergaande inbreuk op (digitale) mensenrechten.

---

[4] International Center for Not-For-Profit Law, «COVID-19, the surveillance pandemic» (https://www.icnl.org/post/analysis/covid-19-the-surveillance-pandemic).

[5] FOC Joint Statement on COVID-19 and Internet Freedom, mei 2020 (https://freedomonlinecoalition.com/wp-content/uploads/2020/05/FOC-Joint-Statement-on-COVID-19-and-Internet-Freedom-1.pdf).

De leden van de PvdA-fractie waarderen het dat het kabinet wijst op het risico van de definitie van cybercrime en de handvatten die een brede definitie aan autoritaire regimes biedt om hun onwelgevallige elementen in cyberspace doelgerichter internationaal op te sporen en te vervolgen. Welke definitie zou volgens het kabinet de te hanteren definitie van cybercrime moeten zijn om dergelijke risico's uit te sluiten? En in hoeverre is het realistisch dat het cybercrime-verdrag van de Raad van Europa universeel zal gaan gelden? Is er al nagedacht over hoe om te gaan met landen die geen deel uitmaken van het Cybercrime-verdrag van de Raad van Europa?

15. Antwoord van het kabinet

In de discussies binnen internationale fora komt naar voren dat landen verschillende definities van het begrip *cybercrime* hanteren. De Cybercrime-conventie van de Raad van Europa bevat geen definitie van cybercrime, maar identificeert verschillende criminele handelingen gerelateerd aan computersystemen, waaronder overtredingen tegen de integriteit en beschikbaarheid van computerdata en -systemen, computer-gerelateerde fraude, verspreiding van kinderpornografie en inbreuken op het auteursrecht. Het definiëren van specifieke criminele handelingen, in combinatie met stevige mensenrechtenwaarborgen en aandacht voor de proportionaliteit van rechtshandhavingsmaatregelen, ziet het kabinet als een manier om risico's van misbruik van internationale instrumenten door autoritaire regimes te ondervangen. Momenteel zijn er 65 landen wereldwijd aangesloten bij de Cybercrime-conventie van de Raad van Europa en meerdere andere landen hebben interesse getoond om partij bij het verdrag te worden. Het kabinet ziet in dat er bij een groep landen zorgen bestaan ten aanzien van de mondiale inclusiviteit van de Cybercrime-conventie van de Raad van Europa. Desalniettemin is het, in het kader van de recent door de Russische Federatie geïnitieerde VN-onderhandelingen over een nieuw cybercrime-verdrag, van belang om op internationaal niveau duplicatie en ondermijning van de bestaande juridische instrumenten te voorkomen. In dat opzicht maakt Nederland zich samen met gelijkgezinde landen ook sterk voor consensus-besluitvorming bij de VN in Wenen, transparantie, inclusiviteit en actieve deelname van het maatschappelijk middenveld en de private sector.

Het kabinet geeft aan dat de waarborging van mensenrechten in het digitale domein plaatsvindt in allerlei processen, maar voor Nederland bovendien vorm krijgt via de Nederlandse inbreng in de Mensenrechtenraad (MRR). De leden van de PvdA-fractie constateren dat de digitale ruimte een cruciaal onderdeel is geworden van de vrijheid voor vereniging, vrijheid van organisatie en vrije meningsuiting. Zo kunnen onder meer organisaties die opkomen voor vrouwenrechten in het digitale domein vrijelijk praten over onderwerpen op een manier waarop ze dat in veel gevallen niet offline kunnen. Tegelijkertijd is het digitale domein ook een plaats geworden voor onderdrukking, een plaats waar activisten of organisaties bewust in kwaad daglicht gesteld worden te doen, waar digitale surveillance plaatsvinden of accounts van activisten onterecht verwijderd worden. In het bijzonder vrouwenrechtenorganisaties of activisten zijn extra kwetsbaar omdat samenlevingen met een bestaande offline vrouwonvriendelijke – en verkrachtingscultuur, deze online voortzet. Welke mogelijkheden ziet het kabinet om deze groepen te beschermen? Valt dit onder de definitie van cybercrime zoals het kabinet die voor ogen heeft? Brengt het kabinet deze wijze van mensenrechtenschendingen ook op in de Mensenrechtenraad? Zal Nederland de adoptie

van de vrijheid van internet-resolutie tijdens de VN Mensenrechtenraad in 2021 promoten? Is het kabinet bereid om een vervolg op de VN Mensenrechtenraad-resolutie over nieuwe technologie en mensenrechten in 2021 voor te stellen om nieuwe ontwikkelingen te reflecteren (HRC 41/14)? Is Nederland bereid te participeren in de VN *Roadmap* voor digitale coöperatie en te zorgen voor inclusie van alle relevante stakeholders, inclusief de *civil society*?

16. Antwoord van het kabinet

Zoals in het antwoord op vraag 13 ook is gesteld, is het werk op de implementatie van de *UN Roadmap for Digital Cooperation* niet gelimiteerd tot de deelname van staten. Het maatschappelijk middenveld neemt hier ook aan deel. De implementatie van de *roadmap* vergt initiatieven vanuit de VN zelf en daarbuiten. Het kabinet wijst bovendien op de belangrijke rol van de *UN Tech Envoy* om de inclusiviteit en samenwerking met het maatschappelijk middenveld te waarborgen.

De leden van de PvdA-fractie lezen in de kabinetsbrief dat Nederland werkt aan versterking van de coördinatie en samenwerking met gelijkgezinde landen op het gebied van de technische normen en standaarden waaronder het internet functioneert. Dit om een versplintering van het internet, met bijkomende negatieve gevolgen voor de openheid, vrijheid en veiligheid van het internet tegen te gaan. Eén van de landen die met name genoemd wordt is China. Bij capaciteitsopbouw is hardware en software gemoeid die bij gebruik van Chinese producten gebaseerd is op Chinese standaarden die negatieve gevolgen hebben voor de openheid, vrijheid en veiligheid van het internet. In hoeverre dreigt het gevaar bij de capaciteitsopbouw in met name Afrikaanse landen, waar China een grote rol speelt, van ondermijning van een open, vrij en veilig internet? Wat is hier de inzet van Nederland? En op welke manier zou de EU hier een rol kunnen spelen om ervoor te zorgen dat openheid, vrijheid en veiligheid van het internet ook voor het Afrikaanse continent gewaarborgd kan worden?

17. Antwoord van het kabinet

Het kabinet deelt de zorgen over openheid, vrijheid en veiligheid van het internet op het Afrikaanse continent. Nederland stelt dat aan de orde in de bilaterale cyberdialogen zoals bijvoorbeeld gevoerd met Zuid-Afrika, via zijn betrokkenheid in de GFCE en door samenwerking met de Wereldbank. Zo heeft de jaarvergadering van de GFCE in oktober 2019 plaatsgevonden in Addis Abeba, met de Afrikaanse Unie als gastheer, waarbij vertegenwoordigers uit 40-tal Afrikaanse landen deelnamen. Nederland heeft bij die gelegenheid aangekondigd een bijdrage te geven van € 1 mln aan het trustfund van het *Digital Development Partnership* (DDP) programma van de Wereld Bank. Een tweede bijdrage van € 1 mln volgde in 2020. Dit trustfund heeft in 2020 capaciteitsopbouw mogelijk gemaakt in o.m. Ghana, Malawi, Tanzania, Senegal, Niger, Nigeria, Zuid-Afrika, Oeganda en Angola. De EU ten slotte heeft in haar EU-Afrika Strategie[6] vastgelegd dat zij de digitale transformatie van het continent een impuls wil geven, door toegang tot veilige en betaalbare digitale diensten te helpen mogelijk maken. De *EU Cybersecurity Strategy for the Digital Decade* bouwt dit verder uit.

[6] Joint Communication Towards a comprehensive strategy with Africa, 9.3.2020 JOIN(2020) 4 final.

De leden van de PvdA-fractie merken op dat Nederland in de dialoog, ook met landen die een offensief cyberprogramma tegen Nederland uitvoeren zoals Rusland en China, wil zoeken naar mogelijkheden om samen te werken op gebieden van gedeeld belang zoals bestrijding van cybercrime. In hoeverre bemoeilijkt het deze dialoog in relatie met hetgeen is opgemerkt over de verschillen in de gehanteerde definitie van cybercrime waarbij landen als Rusland en China hier ruimte zien om onder deze noemer onwelgevallige elementen in cyberspace doelgerichter internationaal op te sporen en vervolgen?

18. Antwoord van het kabinet

Het uitwisselen van kennis en informatie met derde landen, zowel multilateraal als bilateraal, kan van toegevoegde waarde zijn in de preventie en bestrijding van cybercriminaliteit. Het aangaan van een dialoog hierover met bijvoorbeeld de genoemde landen kan daarnaast dienen als vertrouwenwekkende maatregel en kan ertoe leiden dat misverstanden en misvattingen voorkomen dan wel verhelderd worden.

De leden van de PvdA-fractie constateren dat de tegenstelling in de kabinetsbrief nadrukkelijk benoemd is: «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». Welke invloed heeft dat op de samenwerking op de gebieden van gedeeld belang, zoals bestrijding van cybercrime met landen zoals Rusland en China en in hoeverre is er wel sprake van gedeeld belang?

19. Antwoord van het kabinet

De negatieve effecten van cybercriminaliteit op maatschappelijke veiligheid, stabiliteit en economische groei/ontwikkeling gelden mondiaal en geven dus grond voor gedeelde belangen in het voorkomen van cybercriminaliteit, het vergroten van de weerbaarheid tegen cyberaanvallen en het versterken van de capaciteit van rechtshandhaving op dat gebied. Nederland legt zowel in bilaterale als in multilaterale contacten consistent nadruk op het feit dat mensenrechten zowel online als offline gelden, en dat rechtshandhaving in dat opzicht altijd gepaard dient te gaan met een gebalanceerde afweging tussen veiligheid en vrijheden.

De leden van de PvdA-fractie hebben begrip voor de inzet van Nederland binnen de *Freedom Online Coalition* voor gezamenlijke verklaringen over onder meer kunstmatige intelligentie en desinformatie. Op dit moment onderzoekt de door het Comité van Ministers van de Raad van Europa ingestelde *Ad Hoc Committee on Artificial Intelligence* (CAHAI) de mogelijkheid van een bindend wettelijk kader voor de ontwikkeling, het ontwerp en de toepassing van kunstmatige intelligentie, gebaseerd op de universele beginselen en normen van de Raad van Europa inzake mensenrechten, democratie en de rechtsstaat. De leden van de PvdA-fractie vragen in hoeverre Nederland gecommitteerd is aan deze op rechten gebaseerde aanpak van de Raad van Europa. Steunt het kabinet dit proces waarin gekeken wordt naar de haalbaarheid van een wettelijk kader voor de ontwikkeling van en toepassing van artificiële intelligentie die is gebaseerd op de standaarden van de Raad van Europa op het

gebied van mensenrechten, democratie en rechtsstaat? Onderschrijft het kabinet het belang van een dergelijke wettelijke kader?

20. Antwoord van het kabinet

Het kabinet staat een mensgerichte benadering van kunstmatige intelligentie (AI) voor, waarbij de mogelijkheden van AI ten volle worden benut en respect voor publieke waarden (zoals democratie en rechtsstaat) en mensenrechten het uitgangspunt vormen.[7] De ontwikkeling en de toepassing van AI worden reeds genormeerd door een (inter)nationaal wettelijk kader, zoals de diverse mensenrechtenverdragen binnen de Raad van Europa, EU-besluiten over onderwerpen als gegevensbescherming (AVG) en gelijke behandeling en nationale wetgeving zoals de Algemene wet bestuursrecht (Awb). Dit neemt niet weg dat het denken over de (nadere) normering van AI doorgaat. In dit verband verwijst de Kamerbrief van 20 november jl.[8] niet alleen naar het door de leden van de PvdA-fractie genoemde onderzoek in het verband van de Raad van Europa (door de CAHAI), maar ook naar de voorstellen van de Europese Commissie, welke naar verwachting nog dit kwartaal zullen worden gepresenteerd, in opvolging van het Witboek over AI[9]. Het proces rondom CAHAI zal naar verwachting eind 2021 worden afgerond. Nederland neemt actief deel aan in dit proces.

Tevens heeft het kabinet eerder een adviesaanvraag ingediend bij de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) naar de impact van AI.

---

[7] Zie in het bijzonder de «Beleidsbrief AI, publieke waarden en mensenrechten» van 8 oktober 2019, Kamerstuk 26 643, nr. 642.

[8] Zie de «Kabinetsreactie op een drietal algoritmen onderzoeken» van 20 november jl., p. 7. (Kamerstuk 26 643, nr. 726).

[9] Zie: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Zie ook de kabinetsappreciatie van het Witboek over AI: Kamerstuk 26 643, nr. 680.