Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

33 694 Internationale Veiligheidsstrategie

Nr. 52

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 15 november 2019

De vaste commissie voor Buitenlandse Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Buitenlandse Zaken over de brief van 5 juli 2019 over Internationale rechtsorde in het digitale domein (Kamerstuk 33 694, nr. 47).

De vragen en opmerkingen zijn op 2 oktober 2019 aan de Minister van Buitenlandse Zaken voorgelegd. Bij brief van 11 november 2019 zijn de vragen beantwoord.

De voorzitter van de commissie,
Pia Dijkstra

Adjunct-griffier van de commissie,
Konings

kst-33694-52
ISSN 0921 - 7371
's-Gravenhage 2019

Inhoudsopgave **Blz.**

Vragen en opmerkingen vanuit de fracties en reactie van de Minister

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de Kamerbrief over de internationale rechtsorde in het digitale domein. Wel hebben deze leden nog enkele vragen.

De leden van de VVD-fractie vragen de Minister wat de stand van zaken is met betrekking tot het cybersanctieregime waarover recent een akkoord is bereikt. Wanneer kunnen deze leden de implementatie van dit regime verwachten?

1. Antwoord van het kabinet:
Dit regime is in mei 2019, mede op initiatief van Nederland, tot stand gekomen. Nederland is voorstander van zo spoedig mogelijke ingebruikname van dit regime door het plaatsen van personen of entiteiten verantwoordelijk voor cyberaanvallen op de lijst en werkt momenteel in EU-verband aan de precieze invulling.

De leden van de VVD-fractie vragen de Minister verder welke plek het Tallinn Manuel, of diens opvolger, binnen de internationale gemeenschap, en de NAVO in het bijzonder, heeft gekregen. Hoe kijkt de Minister naar de ontwikkelingen, anders dan de conclusies?

2. Antwoord van het kabinet:
De Tallinn Manual 2.0 wordt in het algemeen gezien als een gezaghebbend handboek. Het is uitdrukkelijk geen juridisch bindend document. Geregeld wordt er naar dit handboek verwezen door zowel academici als door overheden en de Talinn Manual fungeert in internationale overleggen vaak als referentiepunt. Het weerspiegelt overigens vaak meerdere standpunten per onderwerp. Dit neemt niet weg dat het aan staten zelf is om duidelijkheid te scheppen over de toepassing van het bestaande internationaal recht in het cyberdomein.

De leden van de VVD-fractie vragen de Minister tot slot welk beleid de NAVO op dit moment hanteert ten aanzien van de toepassing van artikel 5 van het NAVO-Handvest op een cyberaanval door een statelijke dan wel niet-statelijk actor.

3. Antwoord van het kabinet:
Zowel statelijke als non-statelijke actoren kunnen een gewapende aanval plegen in de zin van het VN Handvest. Ten aanzien van digitale aanvallen geldt hetzelfde regime als voor het gebruik van geweld in het fysieke domein. De Noord-Atlantische Raad heeft bepaald dat artikel 5 van het NAVO-verdrag ook van toepassing is op het digitale domein. De inwerkingtreding van artikel 5 is altijd onderwerp van politieke besluitvorming en

wordt van geval tot geval beoordeeld. Voor eventuele collectieve reactie op een aanval geldt dat een beslissing hierover via de bestaande procedures genomen zal worden.

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben met grote belangstelling kennisgenomen van de brief over de internationale rechtsorde in het digitale domein. Deze leden danken de Minister voor deze uitgebreide en heldere uiteenzetting van de dilemma's van de toepassing van het internationaal recht in het digitale domein. Zij hebben nog enkele vragen en opmerkingen.

De leden van de D66-fractie zijn verheugd dat de Minister een leidende rol wil spelen bij het toepassen en versterken van een internationaal normatief kader voor de regulering van cyberoperaties tussen staten. Zeker omdat er momenteel onvoldoende internationale overeenstemming is over de internationale normen en waarden die gelden in het digitale domein. Deze leden constateren dat er sprake is van een grote hoeveelheid cyberaanvallen tussen staten met verschillende doeleinden, van economische spionage tot pogingen tot sabotage van vitale infrastructuur. Deelt de Minister de mening dat deze ontwikkeling van steeds meer en ingrijpendere digitale aanvallen tussen staten een onwenselijke ontwikkeling is en dat Nederland gebaat is bij een goed functionerende internationale rechtsorde die zorgt voor voorspelbaarheid, stabiliteit en conflictpreventie?

4. Antwoord van het kabinet:
Ja. Zoals beschreven in de jaarverslagen van de inlichtingen- en veiligheidsdiensten en het Cyber Security Beeld Nederland (CSBN) (Kamerstuk 26 643, nr. 614) neemt de digitale dreiging toe. Nederland wordt geconfronteerd met uiteenlopende vormen van digitale aanvallen. Zowel statelijke als non-statelijke actoren hebben er baat bij en zijn technisch in staat om collectieve voorzieningen en vitale processen van de overheid en het bedrijfsleven te treffen met gerichte aanvallen.
Door in alle relevante internationale fora actief in te zetten op verheldering van de toepassing van het bestaand internationaal recht op cyberoperaties draagt Nederland bij aan een grotere mate van voorspelbaarheid, stabiliteit en conflictpreventie en daarmee aan de bevordering van de internationale rechtsorde in het digitale domein.

De leden van de D66-fractie delen de mening dat het bereiken van overeenstemming over internationale normen en waarden bij kunnen dragen aan die stabiliteit, net als het belangrijke initiatief van een cybersanctieregime. In dat kader is attributie, oftewel de toerekening van een cyberaanval aan een staat of andere actoren, een zeer lastige zaak is vanwege de vele mogelijkheden om de herkomst van een cyberaanval te verhullen en omdat niet veel staten de middelen hebben om goed attributieonderzoek te doen. Deze leden menen dat een internationale attributie organisatie zou kunnen helpen om internationale attributie van cyberaanvallen te verbeteren. Net zoals de Organisatie voor het verbod op chemische wapens (OPCW) onderzoek doet naar de herkomst van chemische aanvallen zou deze organisatie onderzoek kunnen doen naar de herkomst van grote cyberaanvallen zoals Wannacry of notPetya. Is de Minister dit met de leden van de D66-fractie eens en is de Minister bereid hiervoor in zowel EU- als VN-verband te pleiten?

5. Antwoord van het kabinet:
Zoals beschreven in CSBN 2019 is het vaststellen van de actor achter een digitale aanval, oftewel technische attributie, uiterst complex. Het kabinet heeft in de Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS), de Nederlandse Cybersecurity Agenda (NCSA) en de Defensie Cyber Strategie aangegeven in te zetten op het verbeteren van de eigen attributiecapaciteit. Internationale samenwerking gericht op politieke attributie bevindt zich nog in de beginfase. Op dit moment bestaat er nog onvoldoende overeenstemming om tot een gezamenlijk kader voor het politiek attribueren van kwaadaardige cyberoperaties te komen. Daarnaast bestaat nog discussie over de rol van de private sector. Nederland tast in besprekingen met gelijkgezinde landen af hoe zij hierin staan. Ook zet Nederland zich in voor het versterken van de internationale capaciteit voor technische attributie. Internationale multistakeholder initiatieven zoals het Cyber Peace Instituut en mogelijk ook het Global Forum on Cyber Expertise dragen hieraan bij.

De leden van de D66-fractie zijn verheugd met het feit dat de Minister het toenemende belang van het internet voor mensenrechten en de noodzaak van een veilig, open en vrij internet onderstreept en zich hier internationaal voor inzet. Belangrijk onderdeel hierin is tevens de afspraak in het regeerakkoord om als Nederlandse overheid geen hacksoftware in te kopen die tevens aan schimmige regimes verkocht wordt om hun onderdanen en activisten te onderdrukken. In het kader van mensenrechten en de manier waarop digitale technologie ingezet kan worden om mensen te onderdrukken, willen deze leden de Minister graag wijzen op de Saoedische app «Absher». Deze app wordt gebruikt om vrouwen te onderdrukken in Saoedi-Arabië. Via de app kunnen mannelijke gebruikers de informatie van hun familieleden registreren, en toestemming geven of intrekken om te reizen. Ook krijgen mannen een notificatie als een van de geregistreerde paspoorten wordt gebruikt. Deze app is ook veroordeeld door mensenrechtenorganisaties als Human Rights Watch en Amnesty International. Is de Minister bereid Google en Apple aan te spreken op hun verantwoordelijkheid met betrekking tot Absher en deze bedrijven ertoe te bewegen de app te verwijderen uit respectievelijk de Google Play Store en de App Store? Is de Minister tevens bereid zich hiervoor in EU- en VN-verband in te zetten?

6. Antwoord van het kabinet:
Wanneer belanghebbenden vermoeden dat een bedrijf de mensrechtenrichtlijnen van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) niet naleeft, kunnen zij hiervan melding maken bij een Nationaal Contactpunt (NCP) voor de OESO-richtlijnen in het land waar de misstand plaatsvindt. Indien er in het desbetreffende land geen NCP is, kan de melding worden gedaan in het land waar het bedrijf gevestigd is. Alle landen die de OESO-richtlijnen onderschrijven, dienen een NCP in te stellen. Momenteel beschikken Nederland en de Verenigde Staten over een goed functionerend NCP.
Sinds augustus van dit jaar is het in Saoedi-Arabië op basis van nieuwe regelgeving voor een ieder vanaf 21 jaar mogelijk een paspoort aan te vragen en te reizen naar het buitenland. Vrouwen hoeven geen toestemming meer te hebben van een mannelijk voogd. Vrouwen kunnen tevens als «hoofd van het huishouden» worden aangemerkt en als zodanig toestemming geven aan hun zoon/dochter voor aanvraag van paspoort of buitenlandse reis. De autoriteiten hebben aangegeven dat de app Abshar zal worden aangepast op de nieuwe regelgeving. Desalniettemin blijft

Nederland de kritische dialoog voeren met Saoedi-Arabië over vrouwenrechten en andere mensenrechtenkwesties.

De leden van de D66-fractie zijn tot slot van mening dat goede versleuteling van communicatie wereldwijd van groot belang is. Niet alleen vanuit mensenrechtenbelangen, maar ook vanuit economisch belang. Tegelijkertijd zijn veel belangrijke versleutelingsprojecten, zoals OpenSSl (en tal van forks), Let's Encrypt en Signal van essentieel belang voor een veilig, open en vrij internet. Op wat voor manier ondersteunt de Minister dergelijke projecten? In 2017 is het amendement van het lid Verhoeven aangenomen om geld te investeren in dergelijke projecten (Kamerstuk 34 775 VI, nr. 36). Op wat voor manier is vervolg gegeven aan dit amendement?

7. Antwoord van het kabinet:
Het kabinet hecht belang aan open source encryptie. Dit is daarom ook genoemd als één van de maatregelen in de Nederlandse Cybersecurity Agenda (NCSA) waarbij is aangegeven dat het kabinet hiervoor extra middelen vrij maakt. Deze maatregel wordt uitgevoerd door onder andere het uitzetten van een call onder de Nationale Wetenschapsagenda die is toegespitst op encryptie. Deze wordt binnenkort gepubliceerd. Daarnaast voert de Nationaal Coördinator Terrorismebestrijding en Veiligheid de motie Verhoeven inzake open source encryptie uit. In dat kader wordt een subsidie van € 410.000,- ter beschikking gesteld aan de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO). Met deze subsidie beoogt het kabinet onderzoek te stimuleren op het terrein van encryptie. Het NWO zal binnenkort een uitnodiging tot het indienen van voorstellen publiceren.

Vragen en opmerkingen van de leden van de GroenLinks-fractie

De leden van de GroenLinks-fractie hebben kennisgenomen van de onderhavige brief en de bijgevoegde uiteenzetting over internationaalrechtelijke regels in het digitale domein. Deze leden zijn positief over het streven van de Minister om internationale afspraken over gedragsnormen in het cyberdomein tot stand te brengen en over het instellen van het EU-cybersanctieregime op Nederlands initiatief.

De Minister geeft aan te streven naar het ontwikkelen van internationale afspraken over *vrijwillige, niet-bindende* gedragsnormen voor staten in het digitale domein. De leden van de GroenLinks-fractie vragen waarom de Minister niet een ambitieuzer doel voor ogen heeft, zoals een internationaal cyberverdrag dat wél juridisch-bindend is. Ziet de Minister een kans voor een bindend internationaal cyberverdrag op kleinere schaal – zoals binnen de G7? Zo nee, waarom niet? Kan de Minister zich binnen de United Nations Group of Governmental Experts verder inzetten voor internationale bindende afspraken, toegespitst op cyberaanvallen?

8. Antwoord van het kabinet:
Zoals uiteengezet in de Kamerbrief «Internationale rechtsorde in het digitale domein» die ik op 5 juli jl. naar uw Kamer stuurde, zet het kabinet zich internationaal in voor versterking van de internationale rechtsorde in het digitale domein. Het bestaande internationaal recht is daarbij het uitgangspunt.

Door in te zetten op verheldering van de toepassing van het bestaand internationaal recht op cyberoperaties, draagt Nederland bij aan een grotere mate van voorspelbaarheid, stabiliteit en conflictpreventie in cyberspace. Daarmee levert

Nederland een bijdrage aan bevordering van de ontwikkeling van de internationale rechtsorde. Daarnaast beijvert Nederland zich voor erkenning en implementatie van de aanvullende, niet bindende gedragsnormen, die door de United Nations Group of Governmental Experts (2015) zijn opgesteld en complementair zijn aan bestaand internationaal recht. Op het moment dat staten deze normen in praktijk brengen en hierbij structureel aangeven dat het gaat om juridisch bindende regels, kan dat op termijn leiden tot de ontwikkeling van gewoonterecht.

Momenteel zijn het vooral Rusland, China en hun medestanders die de noodzaak zien voor een nieuw verdrag. Hun doelstelling is om hiermee een centralere rol voor overheden bij het toezicht op het internet te verwerven. Het starten van lange, slepende verdragsonderhandelingen creëert niet alleen rechtsonzekerheid voor de huidige situatie maar er is bovendien een reëel risico dat de verworvenheden onder het huidige internationaal recht te niet worden gedaan. Nederland ziet op dit moment dus geen noodzaak voor een verdrag en richt zich op verduidelijking, toepassing en betere naleving van het bestaand normatief kader.

Nederland is geen lid van de G7, maar zet zich in kleiner verband van gelijkgezinde landen in om de discussie over verantwoord gedrag in cyberspace verder te brengen. Zo heb ik in de week van de Algemene Vergadering van de Verenigde Naties een «Joint Statement On Advancing Responsible Behaviour in Cyberspace» gepresenteerd met Australië en de Verenigde Staten. Deze Verklaring is vervolgens ondertekend door 26 andere landen en staat nog steeds open voor andere landen om zich aan te sluiten.

Is Nederland voorstander van internationale regels voor de *handel* van cyberwapens?

9. Antwoord van het kabinet:
Ja, Nederland is voorstander van striktere regelgeving voor de internationale handel in cyberwapens. In het Wassenaar Arrangement zijn al een aantal jaar onderhandelingen gaande om software, speciaal ontworpen voor het uitvoeren van militaire cyberoperaties onder exportcontrole te brengen. Nederland zet zich actief in om dit voorstel aan te nemen.

De Minister hecht groot belang aan betrokkenheid vanuit het bedrijfsleven en maatschappelijk middenveld. De leden van de GroenLinks-fractie vragen de Minister op welke wijze het bedrijfsleven betrokken wordt in het versterken van de internationale rechtsorde in het cyberdomein.

10. Antwoord van het kabinet:
Samen met de private sector, de technische gemeenschap, academici en non-gouvernementele organisaties zet de Nederlandse overheid internationaal in op een open, vrij en veilig cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.

De Nederlandse internationale inzet richt zich onder meer op de bestendiging van de internationale rechtsorde door de toepassing van internationaal recht, aanvullende normen voor verantwoord gedrag, vertrouwenwekkende maatregelen tussen staten en de daarvoor benodigde capaciteitsopbouw.

Nederland heeft in 2016 de Global Commission on the Stability of Cyberspace (GCSC) geïnitieerd om de discussie te starten tussen overheden, private sector, maatschappelijk middenveld en academische wereld over normen voor verantwoord gedrag in het digitale domein. De GCSC faciliteert als multistakeholder-platform een inclusieve mondiale discussie over stabiliteit in het cyberdomein. De GCSC zal in het eindrapport, dat op 12 november a.s. wordt gepresenteerd, een aantal aanbevelingen formuleren voor concrete normen, waaronder een norm ter bescherming van de publieke kern van het internet en een norm ter bescherming van verkiezingssystemen.

Tenslotte wordt het internationale bedrijfsleven betrokken door middel van het door Nederland gelanceerde publiek-private Global Forum on Cyber Expertise (GFCE). Het bedrijfsleven draagt in het GFCE middels capaciteitsopbouw initiatieven bij aan het versterken van de mondiale weerbaarheid en de internationale rechtsorde in het cyberdomein.

Wordt het bedrijfsleven ook aangesproken op de verantwoordelijkheid die het heeft in het beschermen van de mensenrechten (zoals het recht op privacy) in het cyberdomein?

11. Antwoord van het kabinet:
In aanvulling op wettelijke kaders hebben bedrijven een maatschappelijke verantwoordelijkheid, ook in de digitale economie. Van bedrijven wordt verwacht dat zij conform OESO-richtlijnen en UN «Guiding Principles on Business and Human Rights», handelen. Dit betekent dat bedrijven in kaart moeten brengen of zij (potentiele) misstanden veroorzaken, hieraan bijdragen of hieraan zijn gelinkt. Daarnaast moeten zij deze risico's voorkomen of mitigeren. Om bedrijven handvaten te bieden liet de Europese Commissie al in 2013 een ICT Sector Guide on Implementing the UN «Guiding Principles on Business and Human Rights» opstellen.
Het kabinet is zich ervan bewust dat de toepassing van de OESO-richtlijnen op digitaliseringsvraagstukken nog veelal onbekend terrein is. Daarom draagt het kabinet bij aan een speciale zitting, welke de OESO over dit onderwerp organiseert op 4 november 2019. Eén van de thema's gaat specifiek over online platforms, sociale media en maatschappelijk verantwoord ondernemen.

In de brief lezen de leden van de GroenLinks-fractie over de rol van diplomatieke en politieke druk als reactie op cyberaanvallen. Kan de Minister een overzicht geven van Nederlands diplomatiek optreden tegen ongewenste statelijke cyberoperaties in de afgelopen vijf jaar?

12. Antwoord van het kabinet:
Nederlandse diplomaten zetten zich doorlopend in bilateraal, multilateraal (EU, VN) en in ad hoc coalities in om de prijs op onverantwoord gedrag in het digitale domein te verhogen.
De Nederlandse diplomatie heeft zich goed gepositioneerd door middel van de organisatie van de Global Conference on Cyber Space in 2015, de daarop volgende initiatieven zoals het Global Forum on Cyber Expertise en de Global Commission on Stability of Cyberspace en lidmaatschap van de UN Group of Governmental Experts over normen voor een veilig cyberdomein. Met de versterking van het diplomatiek netwerk met cyberdiplomaten en diverse bilaterale initiatieven heeft Nederland zich in de

voorhoede van een aantal internationale cyberdiscussies geplaatst.
Recente voorbeelden zijn i) de Nederlandse inzet voor een cybersanctieregime, een nieuwe maatregel in de gereedschapskist van de EU om kwaadwillende actoren aan te pakken, ii) de presentatie van een «Joint Statement On Advancing Responsbile Behaviour In Cyberspace» tijdens de Algemene Vergadering van de Verenigde Naties met Australië en de Verenigde Staten, welke door 26 andere landen is ondertekend en iii) de Europese en brede internationale steun die op 4 oktober 2018 werd uitgesproken voor de veroordeling van de cyberoperatie gericht tegen de OPCW.

De leden van de GroenLinks-fractie vragen de Minister of de instrumenten van het nieuwe cybersanctieregime van de EU al zijn ingezet. Is het regime bijvoorbeeld ingezet bij de grootschalige verspreiding van nepnieuws via sociale media door Russische «trollen» met het doel de recente Europese Parlementsverkiezingen te beïnvloeden?[1]

13. Antwoord van het kabinet:
Dit regime is na opdracht van de Europese Raad in oktober 2018 zes maanden later (mei 2019), mede op initiatief van Nederland, tot stand gekomen. Nederland is voorstander van snelle ingebruikname van dit regime door het plaatsen van personen of entiteiten verantwoordelijk voor cyberaanvallen op de lijst en kijkt momenteel in EU-verband naar precieze invulling. De verspreiding van desinformatie valt echter niet binnen de reikwijdte van het cybersanctieregime. Het regime richt zich specifiek op cyberaanvallen, zoals bijvoorbeeld het zich ongewenst toegang verschaffen tot informatiesystemen. Waar het het tegengaan van desinformatie betreft, richt het beleid van de Europese Commissie zich op het verbeteren van detectie, analyse en gewaarwording; versterkte samenwerking; samenwerking met social media platforms en techbedrijven; en het vergroten van bewustwording en maatschappelijke weerbaarheid.[2] De aanpak van het kabinet is vervat in de Kamerbrief Bescherming Democratie tegen Desinformatie van de Minister van Binnenlandse Zaken en kent drie actielijnen: preventie, de informatiepositie verstevigen en (zo nodig) reactie.[3] [4] De Minister van Justitie en Veiligheid richt zich tevens op de aanpak van statelijke dreigingen, waar online desinformatiecampagnes onderdeel van uit kunnen maken. Dit is uiteengezet in de Kamerbrief Maatregelen tegen Statelijke Dreigingen.[5]

Daarnaast zouden de leden van de GroenLinks-fractie graag de Minister vragen hoe hij zich in NAVO-verband zal inzetten om vijandige cyberoperaties te weren. De Minister geeft aan zich daarvoor «in bondgenoot-

---

[1] Musch, S. (2019, 15 juni). EU: individuele Russische trollen probeerden verkiezingen te manipuleren. *NRC Handelsblad*. Geraadpleegd van (https://www.nrc.nl/nieuws/2019/06/15/russische-trollen-probeerden-europese-verkiezingen-te-beinvloeden-a3963844).

[2] Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation (JOIN(2018) 36 final).

[3] Kamerstuk 30 821, nr. 91.

[4] Tevens is uw Kamer In december 2018 geïnformeerd over het tegengaan van desinformatie en de beïnvloeding van verkiezingen (Kamerstuk 30 821, nr. 51), waarna in januari 2019 een BNC-fiche over het Europese Actieplan tegen desinformatie volgde (Kamerstuk 22 112, nr. 2760). Daarnaast is in mei aan uw Kamer een brief gestuurd over de voortgang van het EU actieplan tegen desinformatie (Kamerstuk 30 821, nr. 74).

[5] Kamerstuk 30 821, nr. 72.

schappelijk verband» sterk te maken. Deze leden horen graag wat dit precies inhoudt.

14. Antwoord van het kabinet:
De NAVO heeft in 2014 besloten dat cyber deel uitmaakt van de collectieve verdedigingstaak en dat een cyberaanval de drempel van een gewapende aanval kan overschrijden, en dus kan leiden tot het inroepen van Artikel 5. Tijdens de NAVO-top in Warschau in 2016 erkende de NAVO cyberspace als het vierde domein van operaties (naast lucht, land en zee).
Nederland heeft zich tijdens de NAVO top in 2018 uitgesproken bereid te zijn om eigen cybercapaciteiten in te zetten in het kader van de eigen en bondgenootschappelijke verdediging. Nederland onderschrijft de noodzaak om hier concreet invulling aan te geven.

Is er in NAVO-verband consensus over de toepassing van internationaal recht in het cyberdomein?

15. Antwoord van het kabinet:
De NAVO bondgenoten zijn het met elkaar eens dat het internationaal recht van toepassing is in het cyberdomein. Evenwel houden de NAVO-bondgenoten er hun eigen internationaalrechtelijke traditionele uitgangspunten en opvattingen op na, waardoor er nuanceverschillen zijn, een omstandigheid die overigens niet specifiek is voor het internationaal recht in het cyberdomein. Meningen verschillen bijvoorbeeld over de vraag of het respecteren van de soevereiniteit van andere staten (soevereiniteitsbeginsel) en de verplichting om jegens andere staten gepaste zorgvuldigheid te betrachten (due diligence) eigenstandige, juridisch afdwingbare normen zijn. Sommige staten zijn bijvoorbeeld van mening dat het soevereiniteitsbeginsel zelf geen juridisch afdwingbare verplichting is, maar slechts een beginsel waar andere juridisch afdwingbare normen uit worden afgeleid. Evenzo vinden sommige staten dat gepaste zorgvuldigheid een regel is die geldt binnen een beperkt rechtsgebied, namelijk het internationaal milieurecht, waarvan niet automatisch kan worden aangenomen dat dezelfde regel onverkort in het cyberdomein geldt. Er vindt intensief overleg plaats om samen met bondgenoten en gelijkgezinden dit soort vraagstukken te verkennen en te verduidelijken.

Is er binnen de NAVO belangstelling voor het opzetten van gedragsnormen voor staten in het cyberdomein?

16. Antwoord van het kabinet:
De bondgenoten van de NAVO zetten zich in internationaal verband in voor de toepassing van Internationaal recht en de naleving van vrijwillige niet bindende gedragsnormen zoals aanbevolen door de United Nations Group of Governmental Experts 2015 en ondersteund door de Algemene Vergadering van de Verenigde Naties.

In de bijlage lezen de leden van de GroenLinks-fractie over het interventieverbod. Onder interventie worden ook pogingen om verkiezingen te beïnvloeden in een ander land geschaard. Er staat dat het nog niet volledig is uitgekristalliseerd in het internationaal recht wanneer sprake is van het uitoefenen van dwang. Deze leden vragen de Minister waar hij de lijn trekt wat dit betreft.

17. Antwoord van het kabinet:
Wanneer precies sprake is van dwang, hangt af van de specifieke omstandigheden van het geval en kan niet in algemene zin worden beantwoord. Van dwang is in ieder geval sprake als een operatie wijzigingen veroorzaakt in apparatuur die gebruikt wordt voor verkiezingen. Hiermee wordt de keuzevrijheid van de slachtofferstaat beperkt.

De Minister is van mening dat de bestaande mensenrechteninstrumenten voldoende ruimte bieden om effectieve bescherming van mensenrechten in het cyberdomein te garanderen. De leden van de GroenLinks-fractie vragen de Minister waar hij dit op baseert. Op welke manieren zijn die bestaande instrumenten ingezet om mensenrechten in het cyberdomein te garanderen? Bieden die instrumenten bijvoorbeeld genoeg ruimte om China ter verantwoording te roepen over mensenrechtenschendingen via surveillancesystemen in de regio Xinjiang? En om consumenten te beschermen tegen grootschalige dataverzameling door tech-bedrijven?

18. Antwoord van het kabinet:
Het is belangrijk verschil te maken tussen het bestaan van normen enerzijds en de vraag of staten zich eraan houden anderzijds. Zoals gezegd is het kabinet vooralsnog van mening dat bestaande mensenrechteninstrumenten voldoende handvatten bieden om mensenrechtelijke vraagstukken die opkomen in het cyberdomein, te beantwoorden. Dat deze mensenrechtelijke normen niet altijd worden nageleefd, is betreurenswaardig, maar fundamenteel een probleem dat niet wordt opgelost met nieuwe normen.
Wat de toepassing van surveillance in China betreft ziet het kabinet risico's voor de fundamentele vrijheden, privacy en mensenrechten van Chinese burgers en buitenlandse personen die zich in China bevinden. In Xinjiang is reeds sprake van diepgaande schendingen van privacy en andere mensenrechten door middel van geavanceerde surveillancetechnieken. In de antwoorden op Kamervragen gesteld door u en het lid Kuzu (ingezonden op 3 juni 2019 Aanhangsel Handelingen II 2018/19, nr. 3269) staat een overzicht van recente acties van het kabinet op het Xinjiang-dossier.

De leden van de GroenLinks-fractie hebben ten slotte begrip voor de complexiteit van de attributiekwestie en erkennen het risico van foutieve attributie. Zij vragen de Minister wat de implicaties zijn van foutieve attributie in internationaal recht in het cyberdomein.

19. Antwoord van het kabinet:
Als een staat onterecht een andere staat verantwoordelijk houdt voor een cyberoperatie en daar internationaalrechtelijke consequenties aan verbindt die verder gaan dan onvriendelijke handelingen die niet in strijd zijn met het recht (retorsiemaatregelen), is mogelijk sprake van een internationaal onrechtmatige daad van de attribuerende staat.

Is de Minister voorstander van een internationale organisatie dat onafhankelijk onderzoek doet naar de attributie van cyberaanvallen en attributieclaims verifieert?

20. Antwoord van het kabinet:
Zie antwoord 5 op de vraag van de leden van D66.

Vragen en opmerkingen van de leden van de SP-fractie

De leden van de SP-fractie hebben kennisgenomen van de brief van de Minister over de internationale rechtsorde in het digitale domein. Over de precieze uitwerking van dit internationaal recht hebben deze leden weinig vragen en opmerkingen, maar des te meer over de toepassing ervan en de democratische controle op het gebruik van cyber door staten. Deze vragen vloeien onder andere voort uit het niet beantwoorden van vragen van het lid Karabulut over Nederlandse betrokkenheid bij een cyberaanval tegen Iran, de zogenaamde Stuxnet-aanval (Aanhangsel Handelingen II 2019/20, nr. 387).

De leden van de SP-fractie constateren dat van de tien vragen aan de Minister er enkel één is beantwoord, namelijk vraag 5. Deze leden doen daarom een dringend beroep op de Minister om de negen andere vragen alsnog te beantwoorden. Als de Minister dit opnieuw weigert, vragen deze leden zich af hoe democratische controle op het beleid van de Minister mogelijk is. Kan de Minister aangeven welke ideeën hij hierover heeft? Vindt de Minister het überhaupt problematisch als in een democratie, met daarin de volksvertegenwoordiging als hoogste orgaan, Kamerleden die besluiten moeten nemen over het cyberdomein niet op de hoogte worden gebracht van mogelijke offensieve inzet van dit instrument door de Minister? Is gewaarborgd dat elk offensief gebruik van cyber door Nederland aan de Kamer wordt gemeld? Zo ja, hoe dan? Als dat niet het geval is, waarom dan niet? Graag ontvangen de leden van de SP-fractie een reactie.

21. Antwoord van het kabinet:
De vragen die de leden van de fractie van de SP aan mij hebben gesteld zijn zo volledig als mogelijk beantwoord zonder in te gaan op de operationele inzet van de diensten. Zoals u bekend worden in de openbaarheid nimmer mededelingen gedaan over de operationele activiteiten van de diensten. In voorkomende gevallen dat de Kamer hierover geïnformeerd dient te worden, zal dit via de geëigende kanalen, de Commissie voor de Inlichtingen- en Veiligheidsdiensten, worden gedaan.
Als cybermiddelen onderdeel zijn van de inzet van de krijgsmacht ter verdediging van het eigen grondgebied dan gelden dezelfde kaders als voor de inzet van andere middelen door de krijgsmacht. Als het gaat over de inzet van cybermiddelen ter bevordering van de internationale rechtsorde dan wordt uw Kamer geïnformeerd in overeenstemming met artikel 100 van de Grondwet.

De leden van de SP-fractie kunnen er in het geheel geen begrip voor opbrengen dat de Minister, los van eventuele Nederlandse betrokkenheid hierbij, geen uitspraak wil doen over de mate waarin de Stuxnet-aanval op Iran zich verhoudt tot het internationaal recht. Dit omdat deze aanval waarschijnlijk de meest bestudeerde cyberaanval ooit is, waarover allerlei boeken en artikelen zijn geschreven en juristen zich hebben gebogen. Deze leden roepen de Minister daarom hierop alsnog in te gaan.

22. Antwoord van het kabinet:
Zoals reeds aangegeven zijn de publicaties aangaande de Stuxnet-casus voor rekening van de betreffende journalist, de heer Modderkolk. In dat licht ziet het kabinet ervan af om een uitspraak te doen over de juridische kwalificatie van deze specifieke casus.

Ook vragen de leden van de SP-fractie de Minister voorbeelden te noemen van andere aanvallen of bijvoorbeeld voorbeelden van cyberspionage die (mogelijk) in strijd zijn met het internationaal recht. Vindt de Minister bijvoorbeeld dat de Russische operatie in Nederland gericht tegen de OPCW in 2018, of eerdere hackpoging gericht tegen de Onderzoeksraad voor Veiligheid in 2015, illegaal waren?

23. Antwoord van het kabinet:
In december 2018 heeft Nederland samen met internationale partners de schijnwerper gezet op ondermijnende cyberoperaties door de Russische militaire inlichtingendienst tegen de OPCW. Zoals beschreven in de kamerbrief over verstoring cyberoperatie en veranderende veiligheidsomgeving (Kamerstuk 33 694, nr. 22) heeft Nederland deze uitzonderlijke stap genomen omdat Nederland, als gastland van de OPCW, een speciale internationale verantwoordelijkheid heeft ten aanzien van de integriteit van internationale organisaties in Nederland. Middels deze stappen heeft Nederland die verantwoordelijkheid genomen.

Daarnaast kunnen cyberoperaties het internationaal recht schenden, bijvoorbeeld wanneer een cyberoperatie een internationaal onrechtmatige daad betreft. Op voorhand kan niet worden uitgesloten dat ook cyberspionage een dergelijke onrechtmatige daad oplevert. Dit moet van geval tot geval beoordeeld worden op basis van alle beschikbare informatie.