Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

**26 643** **Informatie- en communicatietechnologie (ICT)**

**30 821** **Nationale Veiligheid**

**Nr. 1080**

**VERSLAG VAN EEN SCHRIFTELIJK OVERLEG**
Vastgesteld 20 oktober 2023

De vaste commissie voor Buitenlandse Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Buitenlandse Zaken over de brief van 9 juni 2023 over de Internationale Cyberstrategie (Kamerstukken 26 643 en 30 821, nr. 1036)

De vragen en opmerkingen zijn op 6 september 2023 aan de Minister van Buitenlandse Zaken voorgelegd. Bij brief van 17 oktober 2023 zijn de vragen beantwoord.

De voorzitter van de commissie,
R. Heerema

De griffier van de commissie,
Westerhoff

kst-26643-1080
ISSN 0921 - 7371
's-Gravenhage 2023

**Inhoudsopgave**



## I Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersoon

### Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met interesse kennisgenomen van de inhoud van de Internationale Cyberstrategie 2023–2028. Hierover hebben zij nog enkele vragen en opmerkingen. De leden van de VVD-fractie hebben een vraag over de constatering bij «doelstelling 1» dat ook cyber-operaties onder de drempel van een gewapend conflict cumulatief het effect kunnen benaderen van de effecten die met een gewapend conflict worden bereikt.

1. Is het kabinet van mening dat de cumulatieve effecten ook significant kunnen zijn als zij een strategisch effect hebben op de geopolitieke machtsverhoudingen, zoals bijvoorbeeld de Noord-Koreaanse campagne om valuta te stelen en zo weerstand te bieden aan VN-sancties tegen haar nucleaire programma? Indien het kabinet deze analyse onderschrijft, is zij van mening dat hiertegen ook, idealiter via coalities van gelijkgezinde landen, opgetreden dient te worden?

**Antwoord van het kabinet**
**Van Noord-Korea is bekend dat het inzet op diefstal van digitale valuta ter financiering van zijn staatskas. Dit is een voorbeeld van de wijze waarop landen cybermiddelen in toenemende mate gebruiken om hun strategische en geopolitieke belangen te dienen. Het kabinet onderschrijft dat Nederland in coalitieverband moet optrekken om tegenwicht te bieden aan landen die door middel van cyberoperaties de belangen van Nederland en bondgenoten schaden. Daarom zet Nederland zich de komende jaren in Europees en NAVO-verband in voor verbetering van de effectiviteit van bestaande instrumenten en het ontwikkelen van additionele strategieën en instrumenten om weerbaarheid en slagkracht te optimaliseren. Tegelijkertijd zal de samenwerking met landen buiten de EU en NAVO verder worden verkend en verdiept.**

2. Ten aanzien van de ambitie proactief op te treden tegen cyberdreigingen vragen de leden van de VVD-fractie of het kabinet het eens is met het standpunt van onder meer Estland dat collectieve tegenmaatregelen in de cybercontext volkenrechtelijk gerechtvaardigd kunnen zijn? Zo nee, waarom niet? Zo ja, hoe is het kabinet van plan dit standpunt uit te dragen en samen met bondgenoten handelingsperspectief te creëren?

**Antwoord van het kabinet**
**Voor het standpunt van het kabinet inzake tegenmaatregelen wordt verwezen naar de Kamerbrief van 13 april 2011, de Kamerbrief van 18 februari 2023 en de kabinetsreactie op het CAVV advies nr. 41.[1] Het kabinet acht tegenmaatregelen in het algemeen belang in ieder geval toegestaan in reactie op een ernstige schending van een regel van dwingend recht, maar zou dit hiertoe niet willen beperken. Volgens het kabinet is het doorslaggevende criterium niet het door de CAVV genoemde «gewicht» van een collectieve verplichting, maar eerder het feit dat er een collectief belang in de naleving bestaat. Dit geldt zowel voor collectieve verplichtingen met een groot gewicht, zoals het verbod op agressie, als collectieve verplichtingen met minder gewicht. Het kabinet zou dus willen aansluiten bij de *International Law Commission* van de VN, die het nemen van maatregelen in het algemeen belang plaatst in het kader van collectieve verplichtingen, en niet uitsluitend van ernstige schendingen van dwingend recht.**
**Nederland heeft dit standpunt uitgedragen in Kamerbrieven, en in internationaal overleg met gelijkgezinde landen. Of een tegenmaatregel in een specifiek geval gerechtvaardigd is, zal moeten worden beoordeeld op basis van de feiten en omstandigheden van dat specifieke geval.**

3. Hierbij vragen de leden van de VVD-fractie ook of het kabinet van mening is dat de cumulatieve effecten van meerdere cyberaanvallen, eventueel begaan tegen meerdere landen in bijvoorbeeld de Europese Unie (EU) of de NAVO, bij elkaar opgeteld kunnen worden om te komen tot één internationale onrechtmatige daad, waarop een collectieve tegenmaatregel genomen kan worden? Vanaf welke vorm zou dit ook onder een «gewapende aanval» vallen, als bedoeld in artikel 5 van het Noord-Atlantisch Verdrag?

**Antwoord van het kabinet**
**Ook een opeenvolgen van handelen of nalaten, kan in aggregaat een onrechtmatige daad vormen. Daarbij is het wel van belang een onderscheid te maken tussen een opeenvolging van handelingen die een cyberaanval vormen tegen één staat, of wanneer deze gericht zijn tegen meerdere staten. In dat laatste geval ontstaat aansprakelijkheid jegens elke aangevallen staat individueel en is geen sprake van één internationaal onrechtmatige daad. Wel zijn alle benadeelde staten dan gerechtigd een tegenmaatregel te nemen en kunnen zij ervoor kiezen dit recht gezamenlijk uit te oefenen.**

**Voor het nemen van tegenmaatregelen in het algemeen belang zie het antwoord op vraag 1.**

**Voor de kwalificatie van een operatie als gewapende aanval wordt gekeken naar de omvang en effecten van de aanval, waaronder het aantal dodelijke slachtoffers, schade en vernietiging. Het kabinet sluit niet uit dat de gevolgen van een reeks van significante cyberoperaties mogelijk samen gekwalificeerd kunnen worden als een gewapende aanval, indien de gevolgen van deze cyberoperaties vergelijkbaar zijn met de gevolgen van een aanval met conventionele wapens. Zoals eerder beschreven in de kabinetsappreciatie over het concept Strategisch Concept**

[1] Kamerstuk 32 500 V, nr. 166; Kamerstuk 35 373, nr. 30.

**van de NAVO van juni 2022[2] hebben NAVO-bondgenoten terecht erkend dat een cyberaanval of een reeks aan kwaadwillende cyberactiviteiten als een gewapende aanval in de zin van artikel 5 gekwalificeerd kunnen worden.**

4. In deze context vragen de leden van de VVD-fractie ook of, gezien de aard van het cyberdomein, het gerechtvaardigd kan zijn om anticiperende tegenmaatregelen te nemen, dus zonder waarschuwing vooraf om de onrechtmatige daad te staken, bijvoorbeeld door ter voorkoming van toekomstige aanvallen verstorende cyberoperaties uit te voeren? Welke ruimte biedt bijvoorbeeld artikel 51 van het VN-handvest hiervoor?

**Antwoord van het kabinet**
**Het nemen van tegenmaatregelen is enkel geoorloofd in reactie op een eerdere schending van een internationaalrechtelijke verplichting door een andere staat. Het nemen van «anticiperende tegenmaatregelen» ter voorkoming van een mogelijke toekomstige schending is dan ook niet toegestaan. Tevens mag een tegenmaatregel niet uit het dreigen met of het gebruik van geweld bestaan.**

**Artikel 51 van het VN-handvest betreft het recht op individuele en collectieve zelfverdediging tegen een gewapende aanval. Het kabinet stelde eerder dat een staat zich mag beroepen op het inherente recht op zelfverdediging wanneer de staat het doelwit is van een cyberoperatie die gekwalificeerd kan worden als een gewapende aanval.[3] Over de reikwijdte van het recht op zelfverdediging bestaat enige discussie, onder meer over de vraag in hoeverre er ook een recht op zelfverdediging bestaat voordat een gewapende aanval heeft plaatsgevonden. Het kabinet deelt de hoofdconclusie van het CAVV en AIV advies uit 2004 dat een land in het geval van een onmiddellijke concreet dreigende gewapende aanval, onder bepaalde voorwaarden een beroep kan doen op het recht van zelfverdediging zoals vervat in artikel 51 van het VN-Handvest.[4]**

5. De leden van de VVD-fractie lezen dat het kabinet inzet op versterking en verduidelijking van de toepassing van het bestaande internationale recht in het cyberdomein. Zij merken op dat het kabinet hier wel een proces beschrijft, maar niet aangeeft hoe het deze normen dan precies ziet. Kan het kabinet hier meer duidelijkheid over geven?

**Antwoord van het kabinet**
**Voor specifieke duiding over de toepassing van het internationaal recht in het cyberdomein verwijst het kabinet naar de bijlage bij de Kamerbrief inzake internationale rechtsorde in het digitale domein van 5 juli 2019.[5] In aanvulling op deze bindende regels bestaat het normatieve kader voor verantwoord statelijk gedrag in het cyberdomein ook uit elf niet-bindende gedragsnormen. Deze hebben onder andere betrekking op cyberactiviteiten gericht tegen kritieke infrastructuur en waardeketens van ICT-producten en diensten.**

---

[2] Zie Kamerstuk 28 676, nr. 408, Kamerstuk 33 000 X, nr. 79 en Kamerstuk 28 676 nr. 196.
[3] Kamerstukken 33 694 en 26 642, nr. 47.
[4] Kamerstuk 29 800 V, nr. 56.
[5] Kamerstukken 33 694 en 26 643, nr. 47.

6. Wanneer is er bijvoorbeeld sprake van een onrechtmatige daad als, ook zonder het gebruik van fysiek geweld, het *domaine réservé* van een staat geschonden wordt door bijvoorbeeld inmenging in nationale verkiezingen?

**Antwoord van het kabinet**
**Er is sprake van een onrechtmatige daad in geval van handelen – of het nalaten van handelen – van een staat, in strijd met een op die staat rustende verplichting onder internationaal recht.**

**Het internationaal recht verbiedt schendingen van de soevereiniteit en het non-interventie beginsel, bijvoorbeeld door inmenging in interne aangelegenheden. Het gaat hierbij om aangelegenheden waarover staten volgens het soevereiniteitsbeginsel zelf de zeggenschap hebben. Nationale verkiezingen zijn een voorbeeld hiervan. Of er sprake is van een van het uitoefenen van dwang, en dus ongeoorloofde interventie, moet per geval beoordeeld worden, maar de essentie is dat het gaat om het bewegen van een staat tot het doen of laten van iets wat die staat normaliter niet vrijwillig zou doen.**

7. En ziet het kabinet bijvoorbeeld de Russische cyberaanvallen op Georgië van 28 oktober 2019 als een onrechtmatige daad?

**Antwoord van het kabinet**
**Indien op grond van de beschikbare feiten de conclusie getrokken kan worden dat er sprake is van onrechtmatig handelen, dan zou Nederland daar, bij voorkeur samen met gelijkgezinde landen, uitspraak over kunnen doen. Het kabinet beoordeelt per geval of dit in het belang is van alle betrokkenen.**

**Tevens wordt in het cyberdomein onderscheid gemaakt tussen verschillende vormen van toerekening (attributie), waaronder technische, politieke en juridische toerekening. Aan de attributie van cyberoperaties ligt altijd een kabinetsbesluit ten grondslag, waarbij wordt gekeken naar de mate van beschikking over eigen informatie dan wel naar een zelfstandig oordeel over verkregen informatie.**

**De cyberaanvallen op Georgië van 28 oktober 2019 zijn middels een diplomatieke verklaring[6] door Nederland veroordeeld en toegerekend aan Rusland.**

8. De leden van de VVD-fractie vragen in deze context ook of het kabinet de analyse deelt dat het duidelijk uitspreken als er sprake is van een onrechtmatige daad, kan bijdragen aan de vorming van internationaal gewoonterecht? Zo nee, waarom niet? Zo ja, is het kabinet bereid in de toekomst dergelijke uitspraken te doen, bij voorkeur samen met gelijkgezinde landen?

**Antwoord van het kabinet**
**In lijn met de Grondwettelijke opdracht aan de regering om de ontwikkeling van de internationale rechtsorde te bevorderen, is het kabinet een voorstander van transparantie over het geldende recht. Daartoe kunnen duidelijke standpunten over de internationaalrechtelijke (on)rechtmatigheid van handelen of nalaten,**

[6] «The Netherlands considers Russia's GRU responsible for cyber-attacks against Georgia», 20 februari 2020, https://www.government.nl/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia

**bijdragen. Tegelijkertijd is het belangrijk alleen veroordelingen uit te spreken indien de feiten daartoe aanleiding geven. Indien op grond van de beschikbare feiten de conclusie getrokken kan worden dat sprake is van onrechtmatig handelen, dan zou Nederland daar, bij voorkeur samen met gelijkgezinde landen, uitspraak over kunnen doen. Desalniettemin zal per geval beoordeeld moeten worden of dit in het belang is van alle betrokkenen.**

9. En is het kabinet van mening dat het uitdragen van een dergelijke opinio juris effectiever kan zijn om langs het gewoonterecht tot normen te komen dan de vruchteloze pogingen om samen met landen als China en Rusland tot een verdrag te komen?

**Antwoord van het kabinet**
**Het kabinet draagt consequent uit dat het internationaal recht van toepassing is in het cyberdomein, waaronder de bestaande regels van internationaal gewoonterecht. Deze regels maken onderdeel uit van het *normatief kader voor verantwoordelijke statelijk gedrag in het cyberdomein* en zijn meermaals bij consensus bekrachtigd in de AVVN. Dit neemt niet weg dat er nog vragen zijn over de precieze toepassing van bestaande regels van internationaal recht in het cyberdomein. Het kabinet stimuleert internationale discussies hierover. Ook zet het kabinet in op het versterken en implementeren van het bestaande normatief kader. Omdat het kabinet van mening is dat het internationaal recht reeds van toepassing is in het cyberdomein, stelt het dat verdragsonderhandelingen over nieuwe regels op dit moment voorbarig en onwenselijk zijn.**

**Vragen en opmerkingen van de leden van de D66-fractie**

De leden van de D66-fractie hebben kennisgenomen van de Internationale Cyberstrategie 2023–2028 en hebben daarover de volgende vragen. Deze leden juichen de ambities die voortvloeien uit de Internationale Cyberstrategie toe, met name als het gaat om het voortouw bij de versterking van de cyberdiplomatie van de EU. Deze leden hechten veel belang aan de steun voor Oekraïne in de oorlog die Rusland al meer dan een jaar geleden is gestart. Hierbij is er ook geregeld sprake van cyberaanvallen door Rusland op verschillende onderdelen van de Oekraïense infrastructuur en de digitale omgeving.

10. De leden van de D66-fractie vragen op welke wijze het Nederlandse kabinet zich inzet voor samenwerking met de Oekraïense cyberinstanties om Russische aanvallen tegen te gaan.

**Antwoord van het kabinet**
**Het Ministerie van Buitenlandse Zaken steunt Oekraïne in het versterken van de cyberweerbaarheid door financiële steun aan een privaat bedrijf, gericht op het mitigeren van cyberincidenten. Het Ministerie van Defensie helpt Oekraïne zich te weren tegen Russische digitale aanvallen op Oekraïense digitale netwerken, waaronder overheden en kritieke infrastructuur. Verder delen EU-partners en andere gelijkgezinde landen kennis en ervaring met Oekraïne, ten behoeve van het versterken van de cyberweerbaarheid.**

Tevens zijn de leden van de D66-fractie van mening dat de oorlog ook de noodzaak tot het tegengaan van toenemende desinformatie met betrekking tot de NAVO heeft blootgesteld. Deze leden vinden het daarom

belangrijk dat het kabinet zich extra inzet om toenemende desinformatie rondom de NAVO tegen te gaan (bijvoorbeeld in de «Global South» en landen rondom Rusland) en hierbij nauwere samenwerking te zoeken met andere bondgenoten binnen de alliantie.

11. De leden van de D66-fractie vragen wat de strategie is voor de privaat-publieke samenwerking om de verspreiding van desinformatie en propaganda tegen te gaan. Welke rol hebben tech-bedrijven volgens de Minister en hoe draagt deze cyberstrategie eraan bij om daartoe te komen?

**Antwoord van het kabinet**
**De platformen van techbedrijven spelen een belangrijke rol in de verspreiding en het tegengaan van desinformatie. Het is voor het kabinet van belang dat de richtlijnen voor het tegengaan van desinformatie niet ingrijpen op de uitoefening van grondrechten, zoals de vrijheid van meningsuiting. Binnen de Europese Unie is hier inmiddels een wetgevend raamwerk voor opgezet, de Digitale Dienstenverordening (Digital Services Act, DSA), waarin deze waarden goed worden afgewogen. Zo moeten grote platformen zelf de risico's van hun diensten in kaart brengen, bijvoorbeeld voor het publieke debat en inzake de verspreiding van desinformatie, en daar passende maatregelen tegen nemen. Deze verplichtingen zijn 25 augustus jl. in werking getreden voor zeer grote online platforms, die onder permanent toezicht zijn komen te staan van de Europese Commissie. Ook hebben lidstaten samen met de Commissie zelfregulering gefaciliteerd, in de vorm van de praktijkcode op desinformatie, die in 2022 is herzien en ondertekend door 34 partijen.**

**In het Commissievoorstel voor de AI-verordening en de raadspositie op die verordening worden gebruikers van deepfaketechnologie verplicht om bekend te maken dat het gegenereerde beeld-, audio- of videomateriaal kunstmatig gegenereerd of bewerkt is. Een dergelijke plicht draagt bij aan het zoveel mogelijk (vooraf) mitigeren van het gevaar dat gemanipuleerd materiaal ten onrechte voor authentiek wordt gehouden. Nederland heeft deze transparantieverplichting in de onderhandelingen in de Raad en in de trilogen met het Europees parlement gesteund. Een mogelijke verdergaande verplichting die is gericht op door AI gegenereerde tekst- of beeldmateriaal waarbij gebruik is gemaakt van auteursrechtelijk materiaal in de trainingsdata, zal door het kabinet bij het Spaanse voorzitterschap onder de aandacht worden gebracht als het onderwerp op de agenda staat.**

De leden van de D66-fractie constateren dat de laatste jaren de invloed van autoritaire regimes op het vrije internet alleen maar is toegenomen, waardoor samenlevingen in verschillende delen van de wereld te maken krijgen met toenemende censuur als het gaat om vrijheid van meningsuiting en persvrijheid, maar ook desinformatie.

12. Deze leden vragen wat de strategie van het kabinet is om deze mondiale risico's voor het vrije internet, in samenwerking met onze bondgenoten, het hoofd te bieden.

**Antwoord van het kabinet**
**De «Freedom on the Net» rapporten laten zien dat internetvrijheid de afgelopen jaren wereldwijd steeds verder is**

**ingeperkt.[7] Om deze zorgelijke ontwikkeling te keren zet het kabinet zich ook de komende jaren, samen met bondgenoten, in voor het aan de orde stellen van online mensenrechtenschendingen in alle internationale fora die zich richten op mensenrechten online. Daarnaast is Nederland in 2024 voorzitter van de *Freedom Online Coalition;* een coalitie van 38 landen.[8] Nederland heeft de ambitie om het lidmaatschap van de FOC te verbreden en thema's aan de orde te stellen zoals *internet governance,* internationaal toezicht op AI technologie en digitale inclusie.**

**Bovendien zet Nederland zich bij de lopende onderhandelingen voor de Europese AI-verordening en het AI verdrag van de Raad van Europa in om bij de ontwikkeling en het gebruik van AI risico's voor onder andere mensenrechten tegen te gaan. Daarnaast is Nederland betrokken geweest bij de totstandkoming van de UNESCO Ethics of AI recommendation.**

**Daarnaast zet het kabinet zich in om – samen met de tech bedrijven, de technologische gemeenschap en academici – het beheer van het internet te borgen. Dit model voorkomt dat één partij de overhand krijgt. Het gezamenlijke beheer van het internet draagt bij aan een vrij en open internet (zie ook het antwoord op vraag 27).**

13. De leden van de D66-fractie zijn voorts benieuwd in hoeverre de uitwisseling van informatie tussen de bondgenoten binnen de EU en de NAVO inzake agressieve cyberstrategie van diverse (non-)statelijke actoren, veilig en beschermd is en niet in handen zal vallen van deze (non-)statelijke actoren.

**Antwoord van het kabinet**
**Informatie-uitwisseling wordt gedaan volgens bestaande voorschriften die verschillen per organisatie. Zowel voor informatie-uitwisseling tussen de EU en haar lidstaten als de NAVO en haar bondgenoten geldt dat er uitgebreide standaarden worden gehanteerd om de authenticiteit, integriteit en vertrouwelijkheid van de informatie te waarborgen. Hierbij zijn interoperabiliteit en veiligheid de belangrijkste elementen. Voor Nederland geldt het hoogste basisbeveiligingsniveau (BBN3). Dat betekent dat er voldaan moet worden aan het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIR-BI) en relevante eisen uit het NAVO-verdrag voor de Beveiliging van Informatie.**

**Vragen en opmerkingen van de leden van de CDA-fractie**

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van de Internationale Cyberstrategie 2023–2028. Deze leden hebben nog enkele vragen en opmerkingen. Zij lezen dat diverse technologische ontwikkelingen, zoals gezichtsherkenningstechnologie en big-data analyse en software, worden misbruikt voor politieke controle.

---

[7] Zie: Freedom House, Freedom on the net: https://freedomhouse.org/report/freedom-net

[8] De Freedom Online Coalitie (FOC) is een diplomatieke coalitie van 38 landen. Mede opgericht door Nederland in 2011, richt deze coalitie zich specifiek op het beschermen en bevorderen van online mensenrechten en internetvrijheid. Leden zijn Argentinië, Australië, Canada, Chili, Costa Rica, Denemarken, Duitsland, Estland, Finland, Frankrijk, Georgië, Ghana, Ierland, IJsland, Italië, Japan, Kenia, de Republiek Korea, Letland, Litouwen, Luxemburg, Maldiven, Mexico, Moldavië, Mongolië, Nederland, Nieuw-Zeeland, Noorwegen, Oostenrijk, Polen, Spanje, Slowakije, Tsjechië, Tunesië, Verenigd Koninkrijk, Verenigde Staten, Zweden en Zwitserland.

14. De ontwikkeling van nieuwe technologieën, zoals AI en quantumtechnologie, zullen ook leiden tot nieuwe risico's voor mensenrechten en democratie. Deze leden lezen echter in de strategie niks over mogelijke exportrestricties op dergelijke nieuwe technologieën die kunnen worden ingezet voor mensenrechtenschendingen. In het recente verleden bleek dat Europese en Nederlandse bedrijven surveillancetechnologieën leveren aan China[9]. Zijn exportrestricties een beleidsoptie, vragen deze leden.

**Antwoord van het kabinet**
**De discussie over exportrestricties op nieuwe technologieën alsmede surveillancetechnologie vindt plaats in de multilaterale exportcontroleregimes en de EU. Alle exportcontroleregimes werken met technische lijsten van goederen en technologieën, welke jaarlijks worden bijgewerkt en in de Europese Dual Use verordening worden overgenomen. Het uitoefenen van controle op de export en het gebruik van bepaalde technologieën heeft zijn grondslag in het Wassenaar Arrangement (WA).[10] Het kabinet zet zich nadrukkelijk in voor het internationaal aan de orde stellen van nieuwe technologieën in relatie tot zorgen over mensenrechtenschendingen binnen exportcontrole van strategische goederen. De herziene EU Dual-Use Verordening, die op 9 september jl. in werking is getreden, draagt bij aan dat uitgangspunt. Deze EU verordening voorziet in een grotere rol van mensenrechten binnen exportcontrole en bevat, mede naar aanleiding van Nederlandse inzet, een expliciete uitbreiding van controles op de export van cybersurveillancetechnologie.**

15. De leden van de CDA-fractie zijn ook benieuwd naar de stand van zaken omtrent samenwerking op het gebied van de ontwikkeling van nieuwe technologieën tussen Nederlandse universiteiten en laboratoria en onderzoekers uit landen waar de mensenrechten digitaal worden geschonden.

**Antwoord van het kabinet**
**Het kabinet werkt samen met de kennissector aan een brede aanpak van kennisveiligheid. Daarin is ook aandacht voor ethische kwesties in internationale wetenschappelijke samenwerking. We zetten in op vergroting van het risicobewustzijn en van de zelfregulering door de kennissector, onder andere aan de hand van de Nationale Leidraad Kennisveiligheid.[11] Dit najaar stuurt de Minister van OCW een sectorbeeld over de kennisveiligheid bij universiteiten naar uw Kamer, voorzien van een beleidsreactie. Dit sectorbeeld geeft weer hoe ver instellingen zijn met het implementeren van voornoemde Leidraad.**

16. De leden van de CDA-fractie zijn tevens benieuwd naar de rol van satellietverbindingen om het vrije internet in stand te houden. De EU is dit jaar begonnen met de bouw van een eigen netwerk van internetsatellieten om communicatie binnen Europa nog veiliger te maken. Iris2 moet overal in Europa betaalbare internettoegang mogelijk maken en voor beveiligde verbindingen zorgen in geografische gebieden van strategisch belang, zoals het Noordpoolgebied en Afrika. De leden van de

---

[9] Zie bijvoorbeeld Nederlands bedrijf levert surveillancetechnologie aan China. (amnesty.nl)
[10] Het Wassenaar Arrangement is een multilateraal exportcontroleregime waaraan 42 landen deelnemen. Het heeft als doel om transparantie en verantwoordelijkheid te bevorderen bij de overdracht van conventionele wapens en goederen en technologieën voor tweeërlei gebruik (dual-use goederen), oftewel zowel militair als civiel gebruik, om zo bij te dragen aan regionale en internationale veiligheid en stabiliteit.
[11] Bijlage bij Kamerstuk 31 288, nr. 948

CDA-fractie lezen in de Internationale Cyberstrategie niks over deze satellieten en zijn benieuwd welke rol dergelijke satellietverbindingen kan worden toegedicht in het veilig en open houden van het cyberdomein.

**Antwoord van het kabinet**
**Het doel van IRIS2 is om een veilig systeem voor satellietverbindingen te realiseren voor publieke en private gebruikers. Dit systeem moet zorgen voor wereldwijde, veilige, flexibele en weerbare satellietcommunicatiediensten voor de Unie en overheidsinstellingen van lidstaten. Uitrol van een eigen Europees satelliet systeem verkleint de afhankelijkheid van derden voor dit type verbinding. De grondhouding van het kabinet is positief, zie hiervoor het betreffende BNC-fiche.**[12]
**Begin 2023 is de EU-verordening «*Secure Connectivity Programme*» aangenomen, waardoor middelen zijn vrijgemaakt voor IRIS2. Er loopt een aanbesteding van de Commissie voor de bouw en inrichting van deze infrastructuur, de stakeholders zijn momenteel aan zet.**

17. De leden van de CDA-fractie zijn verder benieuwd naar de offensieve cybercapaciteiten van Defensie. In hoeverre is Nederland in staat om grootschalige cyberaanvallen te beantwoorden met countercyberoperaties, vragen deze leden.

**Antwoord van het kabinet**
**Een grootschalige cyberaanval vraagt om een samenlevingsbrede respons om de aanval te pareren en de gevolgen ervan te mitigeren. Het hangt af van de specifieke omstandigheden of, als onderdeel van die respons, een countercyberoperatie mogelijk of wenselijk is. De krijgsmacht beschikt met het Defensie Cyber Commando (DCC) over de capaciteiten om, in samenwerking met de MIVD, offensieve countercyberoperaties uit te voeren.**

18. En kan de Minister uiteenzetten wat er in het Strategische Concept van de NAVO is besloten over de mogelijkheid tot de inwerkingtreding van artikel 5 van de NAVO bij een cyberaanval?

**Antwoord van het kabinet**
**De afschrikkings- en defensiepositie van de NAVO is gebaseerd op een passende mix van nucleaire, conventionele en raketverdedigingscapaciteiten, aangevuld met ruimte- en cybercapaciteiten. Het is defensief, proportioneel en volledig in overeenstemming met internationaal recht. Militaire en niet-militaire instrumenten zullen op een proportionele, coherente en geïntegreerde manier worden ingezet om op alle dreigingen voor de NAVO-veiligheid te reageren op de manier, het tijdstip en het domein van keuze (Artikel 20 Strategisch Concept 2022).**

**Het handhaven van een veilig gebruik van en onbelemmerde toegang tot de ruimte en cyberspace zijn van cruciaal belang voor effectieve afschrikking en verdediging. De NAVO zal haar vermogen vergroten om effectief in de ruimte en het cyberdomein te opereren om het volledige spectrum van dreigingen te voorkomen, op te sporen, tegen te gaan en erop te reageren, met gebruikmaking van alle beschikbare instrumenten. Een enkele of cumulatieve reeks kwaadaardige cyberactiviteiten zou het niveau van een gewapende aanval kunnen bereiken en de Noord-Atlantische Raad ertoe kunnen brengen een beroep te doen op**

[12] Kamerstuk 22 112, nr. 3412

**artikel 5 van de NAVO. De NAVO erkent de toepasselijkheid van het internationaal recht en zet zich in om verantwoord gedrag in het cyberdomein te bevorderen (Artikel 25 Strategisch Concept 2022).**

**Vragen en opmerkingen van de leden van de SP-fractie**

De leden van de SP-fractie hebben kennisgenomen van de Internationale Cyberstrategie. Twee omissies willen deze leden graag benoemen.

19. In de eerste plaats valt het hen op dat er weinig tot geen aandacht wordt besteed aan de macht van de multinationale tech-giganten in het cyberdomein en hoe die macht gebreideld kan worden. Ziet de Minister dat ook? Meent de Minister dat een verwijzing naar de (vrijwillige) OESO-richtlijnen voldoende is? Er wordt in de strategie gesproken over strategische coalities waarin ook bedrijven zitten. Wordt daarmee big tech bedoeld? Zo niet, welk type bedrijven dan wel?

**Antwoord van het kabinet**
**Het kabinet bedoelt met de term *big tech* de kleine groep bedrijven die op mondiale schaal opereren en grote invloed hebben op het digitale- en cyberdomein. De EU speelt een belangrijke rol in het aanpakken van de disproportionele marktmacht die deze groep bedrijven op een aantal terreinen uitoefent. Middels bijvoorbeeld de *Digital Markets Act* (DMA) en *Digital Services Act* (DSA) heeft de Unie belangrijke stappen gezet om deze bedrijven onder democratische controle te brengen. Binnen de EU is het wetgevend instrumentarium aanwezig, maar van belang is ook dat er wereldwijd afspraken worden gemaakt over *big tech*. De vrijwillige OESO-richtlijnen vormen een handvat voor deze afspraken en kunnen worden gebruikt voor het in de praktijk uitvoering geven aan wet- en regelgeving, zoals de DMA en de DSA. Daarnaast zet het kabinet in op de wereldwijde toepassing van de *UN Guiding Principles on Business and Human Rights* door bedrijven en overheden.**

**Het kabinet is van mening dat in het maken van afspraken over de werking van het internet alle belanghebbenden betrokken moeten zijn; zowel overheden, de technische gemeenschap, NGOs, academici en internet bedrijven. Hier vallen de *big tech* bedrijven ook onder.**

20. In de tweede plaats missen de leden van de SP-fractie een herbevestiging van de noodzaak en wenselijkheid van een open overheid en de erkenning van klokkenluiders, ook internationaal. Onder welke pijler van de strategie valt dit?

De erkenning en bescherming van klokkenluiders en de noodzaak en wenselijkheid van een open overheid valt onder de tweede pijler van de strategie: «Versterken van democratische en mensenrechtelijke principes online». Het Kabinet zet zich in voor het recht op informatie, ook online, bijvoorbeeld door het aankaarten van internetafsluitingen in VN-verband. Toegang tot informatie is een belangrijke voorwaarde voor een goed functionerende democratie.

21. In dit verband nemen de leden van de SP-fractie de gelegenheid te baat om de Minister nogmaals te verzoeken om de vrijlating van Julian Assange te bepleiten. Assange is een symbool van de strijd om openheid; de bewering dat zijn onthullingen mensen in gevaar zouden hebben

gebracht is tot op heden hol gebleken. De leden van de SP-fractie ontvangen hierop graag een reactie.

**Antwoord van het kabinet**
**Mediavrijheid en persvrijheid zijn essentieel in een democratie en belangrijke pijlers binnen het Nederlandse mensenrechtenbeleid. In veel landen – ook in Nederland – is het echter strafbaar om welbewust staatsgeheime informatie te openbaren. Nederland staat pal voor de rechtsstaat. Het betreft hier een uitleveringsverzoek tussen twee democratische rechtsstaten zonder Nederlandse betrokkenheid. Nederland heeft vertrouwen in de Britse en Amerikaanse rechtsstaat. Het is niet aan Nederland zich te mengen in de rechtsgang van andere democratische landen.**

**Vragen en opmerkingen van de leden van de PvdA-fractie en de GL-fractie**

De leden van de fracties van GroenLinks en PvdA hebben kennisgenomen van de Internationale Cyberstrategie en hebben enkele vragen aan het demissionaire kabinet. De leden van de fracties van GroenLinks en PvdA lezen dat het demissionaire kabinet vasthoudt aan het bestaande standpunt over encryptie, waarmee het demissionaire kabinet aangeeft het niet wenselijk te achten «om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland en sterke encryptie te stimuleren.»

22. Hoe kijkt het demissionaire kabinet naar de wettelijke vastlegging van de bescherming van en het recht op end-to-end encryptie?

**Antwoord van het kabinet**
**De positie van het kabinet over end-to-end encryptie is beschreven in het kabinetsstandpunt encryptie.[13] Hierin wordt gesteld dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland en sterke encryptie te stimuleren. In de internationale context draagt het kabinet deze conclusie en de afwegingen die daaraan ten grondslag liggen uit. Het kabinet is niet voornemens om deze intentie middels wetgeving vast te leggen.**

De leden van de fracties van GroenLinks en PvdA lezen dat het kabinet zich bewust is van de noodzaak om journalisten te beschermen tegen spionage, intimidatie en vervolging via nieuwe cybertechnologie en restrictief cyberbeleid, zoals internet shutdowns.

23. Welke stappen onderneemt het demissionaire kabinet om journalisten wereldwijd te beschermen tegen spionage-software, zoals Pegasus? De leden van de fracties van GroenLinks en PvdA lezen dat de Internationale Cyberstrategie geen enkele passage bevat over de bescherming van online anonimiteit.

**Antwoord van het kabinet**
**Het kabinet is zich bewust van de dreigingen die uitgaan van *intrusion software*. Om deze dreigingen te mitigeren, zijn bepaalde cybersurveillancegoederen en -technologieën onder exportcontrole geplaatst volgens het eerder genoemde**

[13] Zie Kamerstuk 26 643, nr. 383

**Wassenaar Arrangement. Zie hiervoor het antwoord op vraag 14 hierboven.**

**Daarnaast zet Nederland zich internationaal in voor meer controle op cybersurveillancegoederen gerelateerd aan mensenrechtenschendingen. Het beschermen van mensenrechtenverdedigers, waaronder journalisten en advocaten, is een prioriteit. Het kabinet werkt aan exportcontroles op technologie die kan bijdragen aan repressie of mensenrechtenschendingen via de Dual-use Verordening (EU) 2021/821. Door het invoeren van controles op de uitvoer van bepaalde cybersurveillance-items kunnen de risico's op mensenrechtenschendingen doeltreffend worden aangepakt.**

**Verder erkent het kabinet het belang van online anonimiteit als een wezenlijk aspect van digitale privacy en vrijheid van meningsuiting. In lijn met deze erkenning financiert het kabinet organisaties zoals Access Now, die onafhankelijk onderzoek uitvoeren naar *intrusion software*, digitale privacy en veiligheid. Access Now biedt directe ondersteuning aan journalisten tegen digitale dreigingen en bij het waarborgen van hun anonimiteit online.**

**Tegelijkertijd trekt Nederland, als lid en aankomend voorzitter van de *Freedom Online Coalition* nauw op met gelijkgezinde landen op dossiers die raken aan het cyberdomein. Zo publiceerde de *Freedom Online Coalition* in maart 2023 de verklaring *«Guiding Principles on Government Use of Surveillance Technologies»*[14], die illustreert hoe regeringen verantwoord gebruik van surveillancetechnologie kunnen maken, in overeenstemming met internationaal recht en mensenrechten.**

24. Kan de Minister aangeven of het demissionair kabinet van mening is dat online anonimiteit beschermd moet worden en, zo ja, hoe het demissionair kabinet hiervoor internationaal op de bres gaat?

**Antwoord van het kabinet**
Het kabinet ziet online anonimiteit als een wezenlijk aspect van vrijheid van meningsuiting en toegang tot informatie. Het kabinet maakt zich hier internationaal sterk voor door het belang van online anonimiteit vast te leggen in relevante VN resoluties, internationale gezamenlijke verklaringen en door erover in gesprek te gaan met landen waar online anonimiteit in het geding is.

25. De leden van de fracties van GroenLinks en PvdA maken zich ten slotte zorgen over polariserende algoritmes op sociale media gebaseerd op clicks en interacties, waarvan we weten dat ze mensen tegen elkaar opzetten en de verspreiding van haat en desinformatie in de hand werken. Welke stappen onderneemt het demissionaire kabinet om deze algoritmes tegen te gaan?

**Antwoord van het kabinet**
**Het kabinet zet zich zowel in nationaal als Europees verband in voor het tegengaan van desinformatie en de verspreiding van illegale content. Het belangrijkste Europese instrument is daarbij de Digital Services Act (DSA), welke op 25 augustus in werking trad voor de 19 grootste online platforms en zoekmachines en**

[14] Hier te vinden: https://freedomonlinecoalition.com/wp-content/uploads/2023/03/FOC_Guiding_Principles_on_Government_Use_of_Surveillance_Technologies.pdf

**vanaf februari 2024 ook geldt voor andere online diensten en platforms. Binnen de DSA moeten controles worden uitgevoerd op de gebruikte algoritmes en hun impact op fundamentele rechten en het publieke debat, ook door onafhankelijke derde partijen. Daarnaast moeten *service providers* gericht illegale inhoud verwijderen en hun aanbeveling-systemen aanpassen. Gebruikers moeten deze persoonlijke aanbevelingsalgoritmen uit kunnen zetten, en het moet duidelijk zijn op basis waarvan deze algoritmen informatie aanbevelen. Nationaal heeft het kabinet twee actielijnen gedefinieerd voor de aanpak van desinformatie, haatspraak en propaganda. Deze actielijnen worden uiteengezet in de «Rijksbrede strategie effectieve aanpak van desinformatie».[15] Specifiek zet het kabinet in op het versterken van het vrij en open publieke debat, waarbij de nadruk ligt op het behouden van het pluriforme medialandschap; het versterken van de weerbaarheid van burgers en het stimuleren en gebruiken van publieke alternatieven voor online platformen met alternatieve algoritmes die bijvoorbeeld consensus stimuleren, zoals het platform Pol.is.**

**Vragen en opmerkingen van de leden van de ChristenUnie-fractie**

De leden van de fractie van de ChristenUnie hebben met belangstelling kennisgenomen van de Internationale Cyberstrategie. Zij hebben daarover nog enkele vragen. In de Internationale Cyberstrategie wordt opgemerkt dat onze nationale veiligheid, ons verdienvermogen en de veilige online omgeving van de burger op dagelijkse basis worden bedreigd door statelijke en criminele actoren.

26. Deze leden zouden graag een overzicht krijgen van de belangrijkste (voorbeelden van) dreigingen waar Nederland daadwerkelijk mee te maken heeft gehad, voor zover dit mogelijk is.

**Antwoord van het kabinet**
**Het kabinet verwijst naar het recent gepubliceerde Cyber Security Beeld Nederland 2023 (CSBN).[16] Hierin staan verschillende digitale dreigingen vermeld waarmee Nederland te maken heeft (gehad). Het afgelopen jaar waren cyberaanvallen voornamelijk afkomstig van statelijke en criminele actoren en uitval van digitale processen deed zich relatief vaak voor. Volgens het CSBN hebben er in de afgelopen rapportageperiode onder andere ransomware-aanvallen, DDoS-aanvallen van hacktivisten en datalekken door kwaadwillenden en niet-moedwillig menselijk handelen voorgedaan in Nederland. Naast verdere voorbeelden voorziet dit CSBN ook in voorstelbare toekomstige dreigingen voor Nederland, gebaseerd op gebeurtenissen in het buitenland van het afgelopen jaar.**

27. In het document wordt ook opgemerkt dat in de huidige geopolitieke context het «multistakeholder-model» onder druk staat, omdat door verschillende staten wordt gepoogd technische discussies te multilateraliseren waardoor betrokkenheid van maatschappelijke organisaties, de private sector, academici en de technische gemeenschap onder druk komt te staan. Dat heeft ook gevolgen voor het model van het beheer van het internet (*internet governance*). Zou de Minister dit nader kunnen toelichten en kunnen aangeven wat de onwenselijke gevolgen hiervan zijn?

---

[15] Zie Kamerstuk 30 821, nr. 173
[16] Hier te vinden: https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland

**Antwoord van het kabinet**
**Sinds de opkomst van het internet als wereldwijd verbonden netwerk worden de principes, normen en processen die ten grondslag liggen aan het functioneren van het internet ontwikkeld in een multistakeholder-model. De waarde van dit model zit zowel in het bij elkaar brengen van verschillende expertises als in het feit dat een dergelijk model voorkomt dat één stakeholder of staat een dominante rol gaat spelen in het beheer van het internet. Om wereldwijde fragmentatie van het internet te voorkomen is het van groot belang dat het technische beheer van het internet – het beheer en uitgifte van IP-adressen en de technische standaarden die communicatie en interoperabiliteit tussen de netwerken en applicaties faciliteren – gevrijwaard blijft van politieke invloed op de besluitvorming. Echter, indien het beheer van het internet primair een interstatelijke aangelegenheid wordt, is de kans groot dat deze besluitvorming gestuurd gaat worden door geopolitieke belangen. De verwachting is dat dit leidt tot instabiliteit, onzekerheid en in het ergste geval fragmentatie. Zoals in de Internationale Cyberstrategie aangekondigd is, zal het kabinet nader onderzoek laten doen naar de economische gevolgen van fragmentatie op dit technische niveau van *internet governance*. De Minister van Economische Zaken en Klimaat geeft opdracht voor dit onderzoek en verwacht de resultaten hiervan medio 2024 aan uw Kamer te kunnen aanbieden.**

28. De leden van de fractie van de ChristenUnie vragen of de doelstelling om de rol van de EU en de NAVO als internationale cyberactoren te vergroten, de geconstateerde uitdaging dat internationale technische organisaties gepolitiseerd worden, niet verder in de hand zou kunnen werken. Kan de inspraak van de private sector, maatschappelijke organisaties en academici hierdoor juist niet worden beperkt?

**Antwoord van het kabinet**
**Het kabinet is van mening dat deze twee doelstellingen, zowel het vergroten van de rol van de EU en NAVO als het voorkomen van politisering van technische organisaties, elkaar versterken en complementair zijn. Zo leidt een grotere rol van de EU in belangrijke multilaterale (VN-) processen ertoe dat zij steviger kan pleiten voor betekenisvolle deelname van stakeholders uit de private sector, maatschappelijk middenveld, academici en de technische gemeenschap. Een ander voorbeeld is dat het nauwer samenwerken binnen de EU ertoe kan leiden dat het belang van het multistakeholder-model van *internet governance* wereldwijd sterker wordt uitgedragen, bijvoorbeeld door hier op te wijzen in dialogen met derde landen.**
**Tot slot zet het kabinet zich in om ook de deelname van de private sector, maatschappelijke organisaties en academici binnen internationale technische / standaardisatie organisaties te vergroten en te versterken.**

29. Ten aanzien van het versterken van de slagkracht in het cyberdomein zouden de leden van de fractie van de ChristenUnie willen weten welke mogelijkheden de Minister ziet in het bestaande juridische kader om kwaadwillende actoren en hun facilitators (digitaal) op te sporen, aan te pakken, te verstoren en te vervolgen. Is het kabinet van mening dat er ruimere juridische kaders nodig zouden zijn en, zo ja, op welke punten?

**Antwoord van het kabinet**

**De Nederlandse slagkracht in het cyberdomein bestaat uit een combinatie van inlichtingen- en veiligheidsdiensten, rechtshandhavingsmiddelen, militaire capaciteiten en diplomatieke inzet.**

**De AIVD en MIVD werken onder de Wiv 2017, op basis waarvan zij in het kader van hun wettelijke taakuitoefening bijzondere bevoegdheden mogen inzetten. De wettelijke taakuitoefening behelst onder andere het verrichten van onderzoek om de nationale veiligheid te beschermen tegen kwaadwillende (statelijke) actoren in het cyberdomein. Echter, de Wiv 2017 biedt, in de huidige tijd met toenemende cyberdreiging, op punten niet voldoende slagkracht aan de AIVD en MIVD. In de praktijk is gebleken dat zich operationele knelpunten voordoen, waardoor bestaande bevoegdheden niet altijd effectief kunnen worden ingezet en onderzoeken niet goed kunnen worden uitgevoerd. Daarnaast is een statische toetsing- en toezichtstelsel niet passend bij het dynamische karakter van de cyberwereld. Om deze urgente knelpunten in de dagelijkse praktijk van de AIVD en MIVD op te lossen, is een wetsvoorstel[17] ingediend bij de Tweede Kamer, de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma. De Tijdelijke wet moet er voor zorgen dat de AIVD en MIVD hun slagkracht in deze onderzoeken kunnen versterken. Tegelijkertijd wil het kabinet op basis van de Hoofdlijnennotitie, die 1 september (Kamerstuk 34 588, nr. 92) naar de Tweede Kamer is gestuurd, in overleg met de Tweede Kamer, toewerken naar een brede herziening van de Wiv 2017 om de diensten op basis van een toekomstbestendige Wiv beter in staat te stellen op een effectieve manier te opereren, met een daarbij passend stelsel van waarborgen.**

**De krijgsmacht beschikt met het Defensie Cyber Commando (DCC) over offensieve cybercapaciteiten. De krijgsmacht heeft echter geen eigenstandige bevoegdheid om cybercapaciteiten in te zetten tegen kwaadwillende actoren en facilitators. Inzet van de krijgsmacht kan alleen binnen de nationaal- en internationaalrechtelijke kaders en vereist afhankelijk van de specifieke inzet een regeringsbesluit. Ook kunnen onderdelen van de krijgsmacht in het kader van strafrechtelijke handhaving van de rechtsorde bijstand verlenen aan de KMar en politie, of tijdelijk onder de MIVD gebracht worden ten behoeve van haar taakuitvoering onder de Wiv 2017.**

**Inzake verstoring en vervolging in het strafrechtelijke domein geldt dat voor hostingproviders die willens en wetens criminaliteit faciliteren een strafrechtelijke aanpak passend kan zijn. In 2022 heeft het Gerechtshof in Den Haag bepaald dat dergelijke dienstverleners onder omstandigheden niet zijn uitgesloten van strafrechtelijke aansprakelijkheid, ook niet als zij geen bevel tot ontoegankelijk maken van gegevens hebben ontvangen. Deze uitspraak biedt mogelijkheden voor vervolging van hostingproviders die criminelen actief helpen. Aanpassing van het Wetboek van Strafrecht is daarom op dit moment niet voorzien.**

**Naast de mogelijkheden die het strafrecht biedt, is ook de Digitale Dienstenverordening (DSA) relevant. Die verordening verduidelijkt dat een aanbieder van een tussenhandeldienst – die opzettelijk met een afnemer samenwerkt om illegale activiteiten te ontplooien – geen neutrale dienst verricht en daarom niet in**

[17] Zie Kamerstuk 36 263, nr. 2

**aanmerking komt voor de aansprakelijkheidsvrijstellingen neergelegd in de verordening. In dit kader bekijkt de Minister van EZK of er in de memorie van toelichting bij de uitvoeringswet voor die verordening duidelijkheid kan worden gegeven over de kwalificatie van bepaalde hostingdienstverleners en de relevantie van uitspraken zoals die van het Hof Den Haag. Op basis hiervan kunnen het OM, en de ACM als beoogd onafhankelijk toezichthouder op de Digitale Dienstenverordening (DSA), mogelijk samenwerken in de bestrijding van kwaadwillende actoren en hun facilitators.**

**In EU-verband zijn recent belangrijke stappen gezet voor (digitale) opsporing en vervolging. Het *E-evidence* pakket (verordening en richtlijn)[18] maakt de grensoverschrijdende toegang tot elektronisch bewijs sneller en gemakkelijker. Zo worden, met de verordening die in 2026 in werking treedt, rechtstreekse bevelen aan dienstenaanbieders voor het bewaren of verstrekken van gegevens binnen de EU mogelijk. De richtlijn zorgt ervoor dat ook dienstenaanbieders die niet in de EU zijn gevestigd maar wel diensten in de EU aanbieden, deze bevelen kunnen ontvangen en daaraan gehoor moeten geven. Daarnaast maakt ook het 2e Aanvullend Protocol bij het Cybercrimeverdrag van de Raad van Europa (de Boedapest-conventie) het, na ratificatie, mogelijk om rechtstreeks bij dienstenaanbieders elektronisch bewijs op te vragen.**

30. Ten aanzien van de inzet van het cybersanctieregime zouden deze leden willen weten wat het vaker inzetten daarvan in de weg staat.

**Antwoord van het kabinet**
**Voor het sanctioneren van personen en entiteiten onder het EU-cybersanctieregime is steun van alle lidstaten noodzakelijk. Daarnaast moeten sancties gebaseerd worden op openbaar beschikbare informatie en kan de noodzaak van vertrouwelijke communicatie tussen lidstaten vertragend werken. Deze factoren kunnen een belemmering vormen voor de inzet van sancties. Het kabinet pleit er voor dat het EU-cybersanctieregime vaker wordt ingezet en dat verdergaande sancties mogelijk moeten worden. Ook zou het cybersanctie-instrumentarium landen-specifieker moeten kunnen worden ingezet.**

31. De leden van de fractie van de ChristenUnie vragen of het tegengaan van schadelijke desinformatie, haatspraak en propaganda eigenlijk wel behoort tot het onderwerp cyberveiligheid? Kan het kabinet dit nader onderbouwen?

**Antwoord van het kabinet**
**De thema's desinformatie, haatspraak en propaganda behoren tot het onderwerp cyberveiligheid omdat de verspreiding ervan veelal binnen het cyberdomein verloopt. Ook is er soms sprake van cyberoperaties om desinformatie, haatspraak of propaganda te creëren of te verspreiden. Vanwege deze digitale aard ligt het aanpakken van de verspreiding van dit soort online *content* beter besloten in het tegengaan van online dreigingen in den brede. Om deze reden heeft het kabinet besloten de onderwerpen samen aan te pakken.**

---

[18] Verordening: PE/4/2023/REV/1 https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32023R1543. Richtlijn: PE/3/2023/REV/1 https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32023L1544.

32. Terecht is er volgens deze leden in de Internationale Cyberstrategie aandacht voor mensenrechten. Zij vinden het ook van groot belang dat mensenrechtenrisico's van nieuwe technologieën in kaart worden gebracht. Op welke manier gaat het kabinet hier de Kamer van op de hoogte houden?

**Antwoord van het kabinet**
**Het kabinet onderschrijft het belang om mensenrechtenrisico's van nieuwe technologieën grondig in kaart te brengen. Het kabinet zet actief in op het identificeren van deze risico's, in het bijzonder voor kunstmatige intelligentie (AI). Onder meer in de onderhandelingen voor de Europese AI-verordening en het AI verdrag van de Raad van Europa worden mensenrechten geborgd. Ook in de *Task Force on AI and Human Rights* als onderdeel van de *Freedom Online Coalition* zet het kabinet actief in op het identificeren van AI risico's. In deze taakgroep werken afgevaardigden van verschillende landen, bedrijven en universiteiten samen om specifiek de risico's van AI ten aanzien van mensenrechten te identificeren en te adresseren. Ook is Nederland een van de hoofdsponsoren van het *Freedom on the Net* rapport van denktank Freedom House. Dit is een jaarlijks rapport dat inzicht biedt in de staat van vrijheden in het digitale domein op wereldwijde schaal. Het rapport, dat eind oktober a.s. gepubliceerd zal worden, focust met name op de mensenrechtenrisico's van AI. Aspecten zoals surveillance, censuur, desinformatie en privacy worden uitvoerig belicht en geanalyseerd in de context van de uitdagingen en mogelijkheden die AI biedt op het gebied van digitale rechten en vrijheden.**
**Uw Kamer zal jaarlijks, voorafgaand aan het zomerreces, geïnformeerd worden over de voortgang van de uitvoering van de Internationale Cyberstrategie.**

33. Ook bij het standaardiseringsproces spelen mogelijke risico's voor mensenrechten en het kabinet wil deze risico's dan ook nauwlettend in de gaten houden, zo lezen deze leden in de brief. Hoe gaat het kabinet dit doen en hoe wordt de Kamer over de bevindingen geïnformeerd?

**Antwoord van het kabinet**
**Het kabinet pleit er bij verschillende standaardisatieorganisaties voor dat er nauwere samenwerking plaatsvindt tussen technische experts en mensenrechtenexperts. Zo zou een analyse van de impact op mensenrechten een basisonderdeel moeten zijn in de ontwikkeling van standaarden voor nieuwe technologieën. Dit is in lijn met het recent uitgebrachte rapport van de *Office of the United Nations High Commissioner for Human Rights* over mensenrechten en technische standaardisatieprocessen.[19] Het kabinet heeft dit rapport verwelkomd en zal zich de komende jaren inzetten voor de uitvoering van de aanbevelingen in dit rapport. Dit houdt bijvoorbeeld in dat er meer ruimte geboden wordt in standaardisatieprocessen voor betekenisvolle deelname van stakeholders, inclusief het maatschappelijk middenveld. Ook gaat het er hierbij om dat standaardisatieprocessen zo open, transparant en inclusief mogelijk vormgegeven worden, zodat nieuwe standaarden vanuit verschillende perspectieven, zowel technisch als maatschappelijk, kunnen worden ontwikkeld.**

[19] A/HRC/53/42 Human Rights and Technical Standard-setting processes for new and emerging digital technologies: https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session53/advance-versions/A_HRC_53_42_AdvanceUneditedVersion.docx

**Idealiter leidt dit ook tot bredere adoptie van aangenomen standaarden, dat in zichzelf positieve (economische) effecten heeft.**
**Uw Kamer zal jaarlijks geïnformeerd worden over de voortgang van de uitvoering van de Internationale Cyberstrategie.**

**Vragen en opmerkingen van de leden van de SGP-fractie**

De leden van de SGP fractie hebben met interesse kennisgenomen van de Internationale Cyberstrategie 2023–2028 en stellen daarover graag de volgende vragen.

34. Welke principes acht het kabinet internationaal erkend en welke principes zijn dan juist omstreden?

**Antwoord van het kabinet**
**Voor de verschillende deelterreinen van het cyberdomein gelden verschillende kaders en principes. Zo is het cybercrime-verdrag van de Raad van Europa (Boedapest Conventie) leidend als het gaat om principes voor internationale samenwerking om cybercriminaliteit tegen te gaan. De Boedapest-Conventie heeft 68 verdragspartijen wereldwijd en deze principes dienen als richtlijn voor de nationale wetgeving van meer dan honderd landen.**

**Met betrekking tot internationale veiligheid is het normatief kader voor verantwoord statelijk gedrag in het cyberdomein leidend. Dit normatief kader bevat onder andere de erkenning dat het internationaal recht van toepassing is in het cyberdomein, inclusief het VN-handvest en universeel erkende mensenrechten. Daarnaast omvat het normatief kader ook 11 niet-bindende normen. Deze normen behelzen vrijwillige afspraken over o.a. de bescherming van kritieke infrastructuur, mensenrechten en het recht op privacy. Het normatief kader is meermaals in de AVVN met consensus bekrachtigd. Het kabinet acht deze principes dus als internationaal erkend en zal deze ook blijven verdedigen. Een internationaalrechtelijk principe dat Nederland als juridisch bindend ziet in het cyberdomein is het zorgvuldigheidsbeginsel (*due diligence*). Het zorgvuldigheidsbeginsel houdt in dat van staten verwacht wordt dat zij bij het uitoefenen van hun soevereiniteit rekening houden met de rechten van andere staten. Staten hebben de plicht om op te treden wanneer zij kennis hebben van het gebruik van hun grondgebied op een manier die de rechten van een derde staat schaadt, bijvoorbeeld door operaties van cybercriminele groeperingen vanaf hun grondgebied. Dit beginsel wordt (nog) niet door alle staten als een bindende regel van internationaal recht in het cyberdomein erkend.**

**De manier waarop het beheer van het internet vormgegeven is, via een multistakeholder-model, is gebaseerd op internationaal erkende principes. Deze zijn vastgelegd in de *Tunis Agenda for the Information Society*[20] uit 2005, waarin onder andere is afgesproken dat *internet governance* gebaseerd is op de volledige deelname van alle stakeholders, binnen hun respectievelijke rollen en verantwoordelijkheden.**

[20] Zie de Tunis Agenda for the Information Society WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 november 2005

**Hoewel soms zelfs met consensus aangenomen, zijn al deze principes niet vanzelfsprekend en staan ze op al deze deelgebieden van het cyberdomein onder druk. Met name de toepassing van internationaal oorlogsrecht en mensenrechten-elementen zijn omstreden.**

35. Wat stelt het kabinet voor om te doen aan Providers en Internet Service Providers (ISP's) die juist niet met politie en justitie werken? Hoe wordt «bulletproof hosting» voorkomen?

**Antwoord van het kabinet**
**Voor het antwoord op deze vraag verwijst het kabinet naar het antwoord op vraag 29 en naar de Kamerbrief van 16 maart 2023[21] waarin de Kamer is geïnformeerd over oplossingsrichtingen om bulletproof hosting tegen te gaan. Dit omvat het ondersteunen van de sector met informatie over criminele handelingen, het geven van het goede voorbeeld als rijksoverheid door het kiezen voor verantwoorde leveranciers van hostingdiensten, en het eventueel aanpassen van wettelijke kaders. Deze laatste oplossingsrichting wordt momenteel door het Ministerie van Economische Zaken en Klimaat verder onderzocht.**

36. Het kabinet geeft aan dat het te vroeg is voor een nieuw verdrag over statelijk gedrag in het cyberdomein en dat de toepassing in de praktijk nog echt bekeken moet worden voor een nieuw verdrag. Hoe verlopen de gesprekken daarover? Wordt er al enige consensus bereikt met gelijkgestemde landen of met Rusland en China?

**Antwoord van het kabinet**
**Het idee van een nieuw verdrag over statelijk gedrag in het cyberdomein is aangevoerd door Rusland in de VN *Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025* (OEWG). Hierin zijn alle VN-lidstaten vertegenwoordigd. Binnen de OEWG en eerdere VN processen is bij consensus erkend dat het internationaal recht van toepassing is in het cyberdomein. Ook zijn elf vrijwillige, niet-bindende gedragsnormen overeengekomen. Dit normatieve kader is meerdere malen bekrachtigd in de Algemene Vergadering van de Verenigde Naties.**

**Rusland – en in mindere mate China – trekken de toepasbaarheid van bestaand internationaal recht in twijfel en stellen voor om verdragsonderhandelingen te starten. Het kabinet sluit ontwikkeling van nieuwe bindende maatregelen op langere termijn niet uit, maar is van mening dat eerst duidelijk moet worden hoe bestaand internationaal recht moet worden toegepast in het digitale domein. Internationale discussies en trainingen over internationaal recht in het cyberdomein dragen bij aan een beter begrip over dit onderwerp. Mede dankzij deze discussies en trainingen spreken steeds meer landen uit verschillende regio's zich uit over de toepassing van specifieke regels. Deze voortgang is ook zichtbaar in het voortgangsrapport van de OEWG uit 2023, waarin bijvoorbeeld de toepassing van het verbod op geweldgebruik door middel van ICTs wederom is bevestigd.**

37. Rusland en China hebben ook een agenda om het tegengeluid in de digitale ruimte tegen te gaan. Dit bemoeilijkt al lang de consensus die nodig zou zijn voor een eventueel nieuw cyberverdrag als opvolger van de

[21] Zie Kamerstukken 29 911 en 26 643, nr. 392

Budapestconventie. Hoe ziet het kabinet de mogelijkheid voor consensus en overeenstemming op de lange termijn? En wat zijn de alternatieven voor een breed gedragen verdrag?

**Antwoord van het kabinet**
**Het kabinet en de EU blijven gecommitteerd aan het proces om te komen tot een gefocust, effectief en mensenrechten-respecterend VN-verdrag binnen het mandaat van het VN *Ad Hoc Committee*. Een dergelijk VN-verdrag zou volgens het kabinet complementair moeten zijn aan het bestaande cybercrime-verdrag van de Raad van Europa (Boedapest-Conventie). Zo zouden beide conventies uiteindelijk naast elkaar kunnen bestaan. Voor het kabinet is het van groot belang dat de toekomstige conventie effectieve instrumenten biedt aan rechtshandhaving en justitie om cybercriminaliteit wereldwijd aan te pakken, terwijl mensenrechten adequaat beschermd worden. Tijdens de afgelopen onderhandelingssessies is gebleken dat een significante groep VN-lidstaten deze doelstelling deelt. Het kabinet is teleurgesteld dat enkele VN-lidstaten, waaronder Rusland, vergaande voorstellen hebben geherintroduceerd die weinig tot geen kans hebben op consensus. Desalniettemin is het kabinet ervan overtuigd dat de grote meerderheid van de VN-lidstaten er belang bij heeft om binnen afzienbare termijn tot overeenstemming te komen over de inhoud van de toekomstige conventie. Naast deze toekomstige cybercrime-conventie in VN-verband werkt Nederland reeds samen met de 67 andere verdragspartijen bij de Boedapest-Conventie en op bilaterale basis middels wederzijdse rechtshulpverlening met derde landen.**

38. Wat voor argumenten gebruiken Rusland en China tegen de deelname van niet-statelijke actoren in VN-discussies?

**Antwoord van het kabinet**
**De betekenisvolle deelname van niet-statelijke actoren aan VN-discussies is voor het kabinet van groot belang. Sommige VN-lidstaten menen dat discussies die betrekking hebben op internationale veiligheidsvraagstukken, zoals cyber, het exclusieve domein is van staten, waar niet-statelijke actoren geen rol in zouden moeten hebben. Echter, een groot deel van de cyberinfrastructuur is in handen van private sector. Zij hebben daarom ook een rol te vervullen in het bevorderen van internationale veiligheid in het digitale domein. Het kabinet is daarnaast van mening dat het juist in discussies over cyber in VN-verband noodzakelijk is om de expertise en visie van de private sector, het maatschappelijk middenveld, de techgemeenschap en academici mee te nemen. Het kabinet vindt het van essentieel belang om ook op VN-niveau met hen in gesprek te gaan en transparantie te bieden.**

39. De leden van de SGP-fractie vragen voorts hoe goed Defensie erin slaagt technisch personeel te werven, op te leiden en te behouden voor «cyber readiness» en voor zowel offensieve als defensieve capaciteit om haar rol in deze strategie te vervullen. Welke rol speelt oefening en ervaring in «cyber readiness» en in offensieve en defensieve capaciteit? Hoe werkt Defensie aan die oefening en ervaring? Kan Defensie wellicht een meer ondersteunende rol bieden bij de politie, als dat bijdraagt aan het opdoen van ervaring?

**Antwoord van het kabinet**

**Om de *cyber readiness* te vergroten, investeert Defensie in de komende periode niet alleen in cybersecurity en militaire cybercapaciteiten, maar ook in zijn inlichtingenpositie en de digitale rechtshandhaving.**

**Het werven en aanstellen van personeel neemt meerdere jaren in beslag. Defensie is bezig om het Defensie Cyber Commando (DCC) een eigen aanstellingsmandaat te geven, in lijn met de motie van het lid Van Wijngaarden (Kamerstuk 35 925 X, nr. 25), zodat de werving van cyberpersoneel efficiënter en sneller kan verlopen.**
**Voor het behoud van personeel zijn en worden er momenteel diverse initiatieven ontwikkeld binnen Defensie, zoals verwoord in de contourenbrief «behouden, binden en inspireren» (BBI). Zo is DCC gestart met een personeelsprogramma waarbinnen de BBI-maatregelen zijn afgestemd op de unieke eigenschappen waar cyberpersoneel over beschikt. Daarnaast heeft het trainingscentrum van het DCC de defensiebrede Cyber Technische Opleiding (CTO) opgezet om defensiemedewerkers op te leiden; dit heeft geleid tot een directe toename van het beschikbare cyberpersoneel.**

**Defensie traint staand en nieuw personeel met een mix van interne en externe opleidingen. Zowel het DCC als het Defensie Cyber Security Centrum (DCSC) oefenen en trainen met de krijgsmachtdelen om de samenwerking, veiligheid en militaire slagkracht in het cyberdomein over de hele breedte te versterken. Naast nationale samenwerking op het gebied van oefenen en trainen neemt Defensie in internationaal verband deel aan verschillende oefeningen, zoals de NAVO-oefening *Locked Shields*.**

**De ontwikkeling van de digitale slagkracht van DCC gebeurt in nauwe samenwerking met de MIVD in Cyber Missie Teams, zodat personeel van MIVD en DCC gezamenlijk ervaring opdoen. De Koninklijke Marechaussee en de Politie werken reeds op meerdere vlakken samen, waarbij onder meer wordt gekeken naar het uitwisselen van kennis, middelen en waar nodig zelfs tijdelijke capaciteit. Daarnaast verlenen de Koninklijke Marechaussee en andere onderdelen van de krijgsmacht op grond van de Politiewet 2012 militaire bijstand aan de politie, waarmee tevens de ervaringsopbouw van Defensiepersoneel wordt bevorderd. Defensie streeft ernaar deze vormen van interdepartementaal samenwerken en oefenen in de loop der tijd uit te breiden.**

40. Bepaalde statelijke cyberdreigingen worden genoemd in de brief, maar blijven toch buiten bereik van oplossingen. Hoe worden de benoemde vrijhavens bestreden?

**Antwoord van het kabinet**
**Om de hybride dreigingen die uitgaan van statelijke actoren het hoofd te bieden is een samenhangende en diverse set aan maatregelen en instrumenten nodig die Nederland in staat stelt zich hiertegen te weren, zowel in het civiele als militaire domein. In de Kamerbrief Aanpak Statelijke dreigingen van november 2022[22] worden de maatregelen en de kaders waarbinnen deze gecoördineerd kunnen worden ingezet, beschreven. De Neder-**

[22] Kamerstuk 30 821, nr. 175

**landse inzet ten aanzien van cybersecuritydreigingen wordt beschreven in de Nederlandse Cybersecuritystrategie en de Internationale Cyberstrategie.**

**De vrijhavens die in de Internationale Cyberstrategie worden genoemd betreffen vrijhavens voor cyber-criminele organisaties. De Nederlandse diplomatieke inzet om cybercrime tegen te gaan richt zich primair op het bestrijden van vrijhavens voor cyber-criminele groeperingen conform het VN-normatief kader en het toekomstige VN cybercrime-verdrag. Bij het VN normatief kader gaat het met name om het implementeren en bevorderen van het *due diligence* principe, dat bepaalt dat staten verplicht zijn om al het mogelijke te doen om te voorkomen dat er cyber-aanvallen vanaf het eigen grondgebied gepleegd worden. Daarnaast doet Nederland actief mee aan de VN-onderhandelingen over een toekomstig verdrag op cybercrime.**

41. In de kabinetsbrief lezen de leden van de SGP-fractie over opsporingsmiddelen voor repressiedoeleinden. Wat kan het kabinet in de toekomst doen tegen spionagesoftware? Hoe kijkt het kabinet naar de verspreiding en het gebruik van spionagesoftware?

**Antwoord van het kabinet**
**Het kabinet erkent de zorgen omtrent de verspreiding en het misbruik van *intrusion software*.**
**Onrechtmatig gebruik van die software, vooral met repressieve intenties tegen burgers, is onaanvaardbaar.**

**Het kabinet zet zich op verschillende manieren in om misbruik tegen te gaan. Bijvoorbeeld via exportcontrole beleid. Cybersurveillancegoederen en -technologieën vallen onder het Wassenaar Arrangement. Bedrijven in de EU moeten daardoor een exportvergunning aanvragen voor levering buiten de EU, die bij mensenrechtenzorgen kan worden geweigerd. Bovendien streeft Nederland naar strengere internationale controles op cybersurveillancegoederen gelinkt aan mensenrechtenschendingen. Via de Dual-use Verordening (EU) 2021/821 implementeert het kabinet controles op technologie die bijdraagt aan repressie, om zo risico's van mensenrechtenschendingen doeltreffend te reduceren. Hierbij wordt goed in ogenschouw genomen dat het rechtmatig gebruik door Nederlandse diensten niet wordt belemmerd, aangezien dit gebruik de bescherming van nationale veiligheid en criminaliteitsbestrijding ten goede komt. Zie tevens het antwoord op vraag 23.**

**Op diplomatiek vlak zet het kabinet zich, via de Freedom Online Coalitie, in om de samenwerking met gelijkgestemde landen te versterken. Samen kunnen deze landen effectievere normen stellen en maatregelen nemen tegen de verspreiding en misbruik van *instrusion software*. Verder verkent het kabinet de mogelijkheid tot deelname aan een initiatief van de Verenigde Staten dat zich richt op het tegengaan van proliferatie en misbruik van commerciële surveillance technologie: het «*Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware*». Ook zal het kabinet, binnen de kaders van de Internationale Cyberstrategie, diverse diplomatieke middelen blijven inzetten om landen die deze technologieën misbruiken aan te spreken, waar mogelijk in EU-verband.**

42. De leden van de SGP-fractie vragen voorts naar de keuze van het kabinet voor de EU, de NAVO of een samenwerking tussen die twee om internationale cyberdiplomatie te bedrijven. Is er een voorkeur voor een bepaalde partner boven de andere of zijn er duidelijk verschillende inzetten en rollen?

**Antwoord van het kabinet**
**Het kabinet zet zowel binnen de EU als binnen de NAVO in op een daadkrachtigere rol van de respectievelijke organisaties in het cyberdomein. Daarnaast wordt ingezet op meer samenwerking tussen de twee organisaties. Bij het vormgeven van de Nederlandse inzet wordt rekening gehouden met de specifieke doelstellingen en rollen die de organisaties hebben.**

43. Welke middelen heeft het kabinet allemaal in het tegengaan van desinformatie, haatspraak en propaganda? In de brief lezen de leden van de SGP-fractie over «Content Moderation», die bij platforms zelf is neergelegd. Wat zijn de andere instrumenten?

**Antwoord van het kabinet**
**Zie antwoord op vraag 25.**

44. In de strategie lezen zij dat landen soms proberen de technische structuur van het internet naar hun hand te zetten en dat fragmentatie ook dreigt. Hoe verloopt het met deze vraag om erkenning van het niet-politieke karakter van de publieke kern van het internet? Lukt dit in VN-verband al, vragen de leden van de SGP-fractie. En is dat genoeg om de publieke kern en technische structuur van het internet onafhankelijk te laten blijven? Of moeten daar nog vervolgstappen uit voortvloeien?

**Antwoord van het kabinet**
**Zowel in het eindrapport van de vorige *UN Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security* van 2021, als in het jaarlijkse voortgangsrapport van de huidige *UN Open-Ended Working Group on security of and in the use of information and communications technologies* van juli 2023, is overeengekomen dat cyberaanvallen die een impact hebben op de algemene beschikbaarheid en integriteit van het internet een groeiende zorg zijn. Ook is in het eindrapport van de OEWG in 2021 door alle VN-lidstaten afgesproken dat deze algemene beschikbaarheid en integriteit gewaarborgd moet blijven, omdat dit erkend is als kritieke infrastructuur. De publieke kern van het internet is het fundament onder deze algemene beschikbaarheid en integriteit en het behoud ervan is daardoor van groot belang om wereldwijde fragmentatie te voorkomen. Het kabinet zal zich de komende jaren internationaal blijven inzetten voor verdere versteviging en uitwerking van deze afspraken. Zo staan het komende jaar de onderhandelingen over het *Global Digital Compact* van de VN op het programma. Dit moet een overeenstemming worden tussen de lidstaten over de toekomst van de digitale wereld. In 2025 staat een evaluatie over de afspraken die gemaakt zijn tijdens de *World Summit on Information Society* (WSIS) in 2005 en 2015 op de agenda, de zogenaamde *WSIS+20 Review*. Deze afspraken vormen nog altijd de kern van hoe het internet mondiaal beheerd wordt en het kabinet zal zich inzetten om deze afspraken te behouden en te verstevigen.**

45. De leden van de SGP-fractie vinden het goed dat het kabinet helpt om Computer Security Incident Response Teams (CSIRT's) op te bouwen en te versterken in belangrijke partnerlanden en opkomende landen. Hoe verloopt dit? En is dit een doorlopend programma of betreft het tijdelijke ondersteuning, waarna het betreffende land verder gaat?

**Antwoord van het kabinet**
**Het NCSC geeft in samenwerking met een externe consultancy-partner uitvoering aan een meerjarig capaciteitsopbouwprogramma. Dit cyber-capaciteitsopbouw-programma wordt gefinancierd door het Ministerie van Buitenlandse Zaken en vormt onderdeel van de uitvoering van de Internationale Cyberstrategie. Het programma heeft focus op drie regio's in de wereld; Westelijke Balkan, ASEAN, Zuidelijk Afrika. Binnen het programma zijn praktische trainingen ontwikkeld, onder meer gericht op *CSIRT maturity* en *CIIP (critical information infrastructure protection)*.**

**Verder draagt het NCSC in EU en internationaal verband in diverse gremia bij aan kennisoverdracht aan andere landen.**

**Vragen en opmerkingen van de leden van de BBB-fractie**

De leden van de BBB-fractie hebben kennisgenomen van de Internationale Cyberstrategie 2023–2028. Zij hebben daarover de volgende vragen en opmerkingen.

46. Deze leden zijn het ermee eens dat een pro-actievere omgang met cyberdreigingen nodig is. Ook merken zij op dat de Minister een set «doorsnijdende beleidsinstrumenten» voorstelt die een stap in de goede richting zijn met in het bijzonder het versterken van bestaande en nieuwe coalities met opkomende landen. Kan de Minister aangeven welke landen zij hieronder zou verstaan en of er ook actief zal worden ingezet op een versterkte cyber-coalitie met bijvoorbeeld digitaal ontwikkelde landen als Taiwan en Israël?

**Antwoord van het kabinet**
**Als onderdeel van de Internationale Cyberstrategie zet het kabinet in op het versterken van bestaande en nieuwe coalities met opkomende landen. Deze beleidsinstrumenten gelden voor alle drie de pijlers van de strategie. In de strategie worden hiermee in het bijzonder drie regio's aangeduid, te weten de Westelijke Balkan, Azië en Oceanië en landen in zuidelijk Afrika. Om slagvaardige internationale coalities te bevorderen, wordt daarnaast informatie-uitwisseling over cyberdreigingen en multilaterale processen uitgebreid met verschillende partners met hoogwaardige capaciteiten. Dit zijn onder andere Japan, Zuid-Korea, Singapore, Australië en Nieuw-Zeeland.**

De leden van de BBB-fractie verwelkomen ook het initiatief inzake (extra) investeren in inlichtingencapaciteiten. Wanneer cyberaanvallen op grote bedrijven of ministeries worden uitgevoerd, krijgt het dikwijls nationale aandacht, maar een sluipender probleem is de kwetsbaarheid van lagere overheden en het midden- en kleinbedrijf (MKB) voor cyberaanvallen. Zij hebben vaak niet de middelen, kennis of het digitale bewustzijn om cyberaanvallen te voorkomen of bestrijden. Genoeg financiële en juridische middelen en bevoegdheden voor inlichtingencapaciteiten kunnen bijdragen aan een meer weerbare en efficiëntere nationale cyberveiligheid, aldus de leden van de BBB-fractie.

47. Wat wil het kabinet specifiek ondernemen om lagere overheden en het MKB weerbaarder te maken?

**Antwoord van het kabinet**
**De inzet van het kabinet op de versterking van de digitale weerbaarheid van het MKB is opgenomen in de Nederlandse Cybersecuritystrategie (NLCS) en de Strategie Digitale Economie. Het Digital Trust Center (DTC) van het Ministerie van Economische Zaken en Klimaat (EZK) speelt hierin een belangrijke rol. Het DTC helpt bedrijven (van grote bedrijven tot zzp-ers) meer digitaal weerbaar te worden tegen cyberdreigingen, dit doet zij op twee manieren. Ten eerste geeft het DTC informatie en advies bijvoorbeeld via haar website en biedt zij verschillende tools aan zoals de Bassiscan Cyberweerbaarheid. Tevens beschikt het DTC over een notificatiedienst. Bedrijven worden dan geïnformeerd over specifieke digitale kwetsbaarheden en dreigingen. Met deze informatie kunnen bedrijven actie ondernemen om schade voor het bedrijf te voorkomen of zoveel mogelijk beperkt te houden. Ten tweede stimuleert het DTC samenwerkingsverbanden van bedrijven in een regio of branche. Hierin kunnen ondernemers van elkaar leren, ervaringen uitwisselen en samenwerken aan producten die helpen om cyberweerbaar(der) te worden. Inmiddels is hierdoor een netwerk van 56 samenwerkingsverbanden ontstaan. U bent op 23 februari jl. door de Minister van EZK geïnformeerd over de voortgang van het DTC. [23] Daarnaast zult u dit najaar worden geïnformeerd over de voortgang van Nederlandse Cybersecuritystrategie (NLCS) en de Strategie Digitale Economie.**

**Het kabinet onderschrijft bovendien de noodzakelijke aandacht voor cyberweerbaarheid van lagere overheden en onderneemt hier reeds vanuit verschillende initiatieven actie op. Zo bevat de Baseline Informatiebeveiliging Overheid (BIO), het basisnormenkader voor informatiebeveiliging bij de overheid, een minimale set aan maatregelen voor overheidsorganisaties voor het verhogen van de digitale weerbaarheid. Het doel hiervan is om te voorkomen dat overheidsorganisaties het slachtoffer worden van digitale aanvallen. De herziening van de Netwerk- en Informatiebeveiligingsrichtlijn (NIS2) geeft handvatten om maatregelen van de BIO wettelijk te verankeren en het toezicht op de gehele overheid, zo ook lagere overheden, in te richten. Deze richtlijn wordt momenteel omgezet in nationale wetgeving. Het toezicht op informatiebeveiliging bij de overheid zorgt dat de noodzakelijke maatregelen zoals benoemd in de BIO op een goede manier worden toegepast. Naast deze initiatieven voor het verhogen van de weerbaarheid wordt ook door overheidsorganisaties, waaronder lokale overheden, geoefend om voorbereid te zijn indien, ondanks de genomen maatregelen, toch incidenten plaatsvinden. Dit doen zij bijvoorbeeld tijdens de jaarlijkse Overheidsbrede Cyberoefening, waar verschillende overheidsorganisaties oefenen met gesimuleerde hackaanvallen. Op deze manier worden bestaande crisisplannen getest in de praktijk en leren organisaties hoe ze moeten handelen tijdens incidenten. Deze Overheidsbrede Cyberoefening is aanvullend op dat wat de verschillende bestuurslagen zelf al organiseren, zoals de oefenpakketten van de Informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten (VNG). Tot slot: het belang dat wordt gehecht aan de versterking van de cyberweerbaarheid**

[23] Kamerstuk 26 643, nr. 980

**van lokale overheden komt ook terug in het Bestuurlijk Convenant Digitale Veiligheid Gemeenten.[24] Hierin worden de uitgangspunten geschetst voor de gezamenlijke inzet op het verbeteren van digitale veiligheid op lokaal niveau door de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Justitie en Veiligheid en de voorzitter van de Vereniging Nederlandse Gemeenten.**

48. Veiligheidsdiensten moeten volgens de leden van de BBB-fractie meer ruimte krijgen om bevoegdheden te gebruiken in hun werk, met daarbij als voorwaarde een wettelijk kader waardoor toezichthouders controles kunnen uitvoeren. Hoe ziet het kabinet een dergelijk juridisch kader?

**Antwoord van het kabinet**
**Voor de AIVD en MIVD geldt, onder verwijzing naar de beantwoording van vraag 29, dat met de Tijdelijke wet, de AIVD en MIVD hun bestaande bevoegdheden effectiever moeten kunnen inzetten, waarbij tegelijkertijd de waarborgen waarmee die inzet moet zijn omgeven op een hoog niveau blijven. Met de Tijdelijke wet wil het Kabinet inzetten op meer dynamisch toezicht, waarbij de toetsing aan de voorkant op enkele punten verplaatst wordt naar bindend toezicht tijdens de uitvoering van bevoegdheden. Hierdoor sluit de aard van het toezicht beter aan bij de fase en de dynamiek van het onderzoek en kan tevens een (voortdurende) rechtmatige uitvoering van de wet worden gemonitord.**

**II Volledige agenda**

– De brief van de Minister van Buitenlandse Zaken van 9 juni 2023 over de Internationale Cyberstrategie (ICS) 2023–2028 (Kamerstukken 26 643 en 30 821, nr. 1036).

[24] Stcrt. 2022, nr. 35231