26 643 VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

30 821 Vastgesteld, xx

Nr. xxx

Binnen de vaste commissie voor Buitenlandse Zaken hebben de onderstaande fracties de behoefte vragen en opmerkingen voor te leggen aan de minister van Buitenlandse Zaken over de brief van 6 december 2024 over de uitvoering van de Internationale Cyberstrategie 2023-2028 (26 643/30 821, nr. 1252).

De op 26 maart 2025 aan de minister toegezonden vragen en opmerkingen zijn met de door de minister bij brief van … toegezonden antwoorden hieronder afgedrukt.

De voorzitter van de commissie,
Klaver

De griffier van de commissie,
Westerhoff

Inhoudsopgave

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de PVV-fractie

De leden van de PVV-fractie hebben kennisgenomen van de kabinetsbrief over de uitvoering van de Internationale Cyberstrategie (ICS). Deze leden hebben enkele vragen en opmerkingen over deze brief.

De inzet van dit kabinet om een open, vrij en veilig digitaal domein te bevorderen kunnen deze leden zeer waarderen. Dat er het afgelopen jaar voortgang is geboekt op de drie strategische doelstellingen, is positief. Wel maken de leden van de PVV-fractie zich zorgen over de komende paar jaar. De laatste maanden zijn er veel panelen gaan schuiven in de internationale politiek. De Verenigde Staten (VS) vraagt meer Europese inzet op het gebied van veiligheid. En op het gebied van defensie gaat er enorm veel geïnvesteerd worden. Ondertussen neemt de dreiging van agressieve cyberactoren toe. Wat hebben deze recente ontwikkelingen voor invloed op het Nederlandse Cyberbeleid? Verandert de Nederlandse diplomatieke inzet? Zo ja, op welke punten?

1. Antwoord van het kabinet

De veranderende geopolitieke verhoudingen dwingen Nederland en Europa om keuzes, inzet en partnerschappen op het gebied van veiligheid opnieuw te bekijken. Dat geldt in het digitale domein evenzeer als in het fysieke domein. De toenemende digitale dreiging die uitgaat van grote statelijke actoren zoals Rusland en China wordt in de Internationale Cyberstrategie uitgebreid besproken. De Trump-regering herpositioneert de VS op vele terreinen, waaronder ook in het cyberdomein. Tegelijkertijd is de samenwerking met de VS op het tegengaan van cyberdreigingen hecht en intensief. Het kabinet zet zich ervoor in bestaande samenwerking zoveel mogelijk te consolideren, en te blijven bezien waar uitbreiding mogelijk en opportuun is.

Het kabinet ziet een doorzettende trend dat steeds meer landen offensieve cyberprogramma's ontwikkelen die gericht zijn tegen Nederland en onze bondgenoten, en dat de dreiging die uitgaat van die programma's omvangrijker wordt.[1] Tegen die achtergrond blijven de doelstellingen uit de Internationale Cyberstrategie (*tegengaan* van cyberdreigingen van staten en criminelen, *versterken* van democratische en mensenrechtelijke principes online en *behouden* van een wereldwijd open, vrij en veilig internet) onverminderd relevant. De context waarbinnen die doelstellingen moeten worden gerealiseerd is echter nog complexer en uitdagender geworden.

De noodzaak voor de EU om meer te investeren in de eigen veiligheid geldt daarom nadrukkelijk ook voor het digitale domein. Daarop worden al belangrijke stappen gezet. Op het gebied van versterking van de Europese weerbaarheid werden recentelijk onder andere plannen inzake een *EU Preparedness Union Strategy* en een Witboek over Europese defensie en *ReArm Europe / Readiness 2030* gepresenteerd.

Op extern vlak is het zaak dat de EU ook meer slagkracht ontwikkelt om landen die offensieve cybercampagnes uitvoeren tegen de EU te ontmoedigen. Dat vereist nauwe afstemming tussen de lidstaten bij de inzet van militaire cybermiddelen en inlichtingen- en verstoringsoperaties. Ook moet de EU als diplomatieke actor zich duidelijker profileren in dit domein via instrumenten als publieke attributies, sancties en het verlenen van (technische) steun aan onze partners binnen en buiten de EU. Nederland speelt in dit proces een voortrekkersrol. De betrekkingen met de VS in dit domein zijn altijd hecht en

[1] Zie in dit kader bijvoorbeeld het Cybersecuritybeeld Nederland 2024 en de meest recente jaarverslagen van MIVD en AIVD.

intensief geweest. Het is in het belang van onze eigen veiligheid die samenwerking zo goed mogelijk te continueren en waar mogelijk en opportuun verder uit te breiden.

Een steviger Europees fundament voor het digitale domein maakt ook dat de democratische en mensenrechtelijke principes online worden geborgd. Met eigen, Europese digitale diensten is Nederland minder afhankelijk van *Big Tech*. Dit beleid raakt aan de beleidsinzet op Digitale Open Strategische Autonomie.

In de brief staat dat Nederland samen met gelijkgezinde landen toewerkt naar een mechanisme van de Verenigde Naties (VN) voor een normatief kader voor verantwoordelijk statelijk gedrag in het cyberdomein. Dat klinkt allemaal redelijk, maar wat is zo'n kader waard in relatie tot landen (zoals China en Rusland) die zich in het cyberdomein zeer onbehoorlijk en agressief opstellen?

2. Antwoord van het kabinet

Het normatief kader voor verantwoordelijk statelijk gedrag is in 2015 opgesteld en in 2021 door alle VN-lidstaten bekrachtigd in de AVVN. Belangrijk onderdeel van het kader is de afspraak dat internationaal recht ook van toepassing is op de digitale wereld (*cyberspace*).[2] Daarnaast omvat het kader een reeks vrijwillige normen, zoals de bescherming van kritieke infrastructuur, het respecteren van mensenrechten en de oproep digitale kwetsbaarheden te rapporten. Omdat het normatief kader door alle VN-lidstaten bekrachtigd is, biedt het een fundament om waar nodig diplomatieke stappen, zoals sancties, te kunnen zetten in geval staten deze normen overtreden. Hoewel het normatief kader geen garantie biedt voor een veilig cyberdomein, geeft het wel de marges voor handelen aan waarover consensus geldt. Bovendien bieden de multilaterale afspraken handvatten om de gesprekken met landen aan te gaan en te intensiveren.

De leden van de PVV-fractie vinden het voorts opvallend dat Zuid-Afrika wordt genoemd als één van de partnerlanden waar Nederland cyberconsultaties mee heeft gevoerd. De president van Zuid-Afrika sprak enkele maanden geleden nog lovend over Poetin en Rusland. Ook hield Zuid-Afrika in 2023 nog een gezamenlijke militaire oefening met Rusland en China. Wat maakt zo'n land dan een belangrijk (en betrouwbaar!) partnerland op cybergebied?

3. Antwoord van het kabinet

Zuid-Afrika is een belangrijke geopolitieke speler en een strategische partner voor Nederland op het Afrikaanse continent. Dit jaar in het bijzonder als voorzitter van de G20. Aangezien cyberveiligheid een grensoverschrijdend thema is, blijft het voor Nederland van belang om de dialoog te voeren met landen als Zuid-Afrika, ook als die niet op alle fronten dezelfde internationale positie innemen. Er zijn veel waarden die Nederland en Zuid-Afrika delen; zo staat Zuid-Afrika bovenaan in de mondiale index van internetvrijheid voor het Afrikaanse continent. Nederland en Zuid-Afrika zijn gelijkgezind als het gaat om de bescherming van mensenrechten online, digitale inclusie en het betrekken van

[2] Zie voor een verdere toelichting op de toepassing van het internationaal recht in het digitale domein kamerstuk TK 2018-2019, 33 694 & 26 643, Nr. 47.

maatschappelijke organisaties, academici en de private sector bij de ontwikkeling van digitaal beleid.

De leden van de PVV-fractie horen daarom graag welke risico's er voor Nederland opdoemen door de ontwikkelingen op het gebied van AI. Deze leden willen specifiek weten of de dreiging die uitgaat van statelijke actoren en criminelen, door de inzet van AI is toegenomen? Zo ja, hoe wordt deze dreiging gepareerd?

4. Antwoord van het kabinet

Op 9 december 2024 heeft de minister van Justitie en Veiligheid uw Kamer een analyse gestuurd van het effect van AI op de nationale veiligheid ('Versterkte dreigingen in een wereld vol kunstmatige intelligentie').[3] Deze stelt dat AI naast kansen ook zeer waarschijnlijk bestaande dreigingen ten aanzien van o.a. economische, territoriale en fysieke veiligheid versterkt en invloed heeft op sociale en politieke instabiliteit. Statelijke actoren gebruiken AI voor het genereren en verspreiden van desinformatie om hiermee andere landen te ondermijnen. De ontwikkeling van AI vergroot ook de cybercapaciteit van diverse actoren, zowel in het militaire domein als daarbuiten. Hoewel de volledige impact van AI op cyberoperaties nog niet kan worden vastgesteld, kan AI momenteel al wel een faciliterende rol spelen bij cyberaanvallen. Zo kan AI worden gebruikt om snel mogelijke doelwitten te selecteren en om *phishing*-mails te genereren.

Een belangrijk risico is bovendien dat AI militaire proliferatie en escalatie in de hand kan werken. Hierbij valt te denken aan een steeds verdergaande versnelling van militaire besluitvorming en uitdagingen op het gebied van defensieve systemen. De werking van defensieve systemen is niet meer vanzelfsprekend vanwege de snelheid waarin nieuwe AI-toepassingen zich ontwikkelen. Tot slot bestaat er het risico dat systemen inadequaat worden ontwikkeld en zo in strijd zijn met het internationaal recht. Alle deze ontwikkelingen brengen ook nieuwe cybersecurity risico's met zich mee.

Nederland zet zich via bestaande en nieuwe internationale samenwerkingsverbanden actief in om veiligheidsdreigingen gerelateerd aan AI tegen te gaan. Zo nam Nederland op 10 en 11 februari 2025 op verschillende niveaus deel aan de *AI Action Summit* in Parijs. De ministeries van Buitenlandse Zaken en Defensie leverden een prominente bijdrage aan een verklaring over het gebruik van AI in het militaire domein.[4] Daarnaast ondertekenden het NCSC en de AIVD gezamenlijk met internationale partners een risicoanalyse[5] over AI en cyberdreigingen wat bijdraagt aan het opbouwen van een gezamenlijk dreigingsbeeld. Ook zijn BZ en Defensie nauw betrokken bij de derde *Responsible AI in the Military Domain (REAIM)*-top die in september dit jaar wordt georganiseerd door Spanje.

De ontwikkelingen rondom kunstmatige intelligentie (AI) zijn het afgelopen jaar in een stroomversnelling geraakt. Net als met andere technologische ontwikkelingen uit het verleden, brengen nieuwe technologieën risico's met zich.

[3] Kamerbrief bij analyse van het effect van AI op de nationale veiligheid, Kamerstuk 30821, nr. 252
[4] Paris Declaration on Maintaining Human Control in AI enabled Weapon Systems. | Élysée
[5] Building trust in AI through a cyber risk-based approach | ANSSI

Is het kabinet met deze leden van mening dat meer internet governance kan leiden tot een beperktere vrijheid van meningsuiting? Zo ja, wat gaat Nederland doen om een beperking van de vrijheid van meningsuiting te voorkomen?

5. Antwoord van het kabinet

De term "*internet governance*" wordt gebruikt wanneer het gaat over afspraken over het internet zelf, waaronder het beheer en uitgifte van IP-adressen en domeinnamen, en de technische standaarden die communicatie en interoperabiliteit tussen de netwerken en applicaties faciliteren. Indien deze afspraken op een staatsgeleide en gesloten manier worden gemaakt, zoals o.a. Rusland en China willen, dan is er een risico op inperking van de vrijheid van meningsuiting online. Sommige staten hebben in het verleden technische standaarden voorgesteld die bijvoorbeeld censuur en statelijke controle op het internet vergemakkelijken. Nederland werkt samen met gelijkgezinde partners om dit tegen te gaan en mensenrechten en democratische beginselen te borgen in technische standaarden voor het internet en digitale technologieën. Ook bieden we tegendruk wanneer technische standaarden voorgesteld worden die een risico vormen voor mensenrechten, inclusief de vrijheid van meningsuiting online.

Nederland zet zich in voor het tegengaan van internet shutdowns, censuur en surveillance. Voor de leden van de PVV-fractie zijn dat belangrijke punten. Deze leden zullen in het verlengde daarvan erop blijven letten dat de vrijheid van meningsuiting ruimte blijft krijgen in het digitale domein. Wat dat betreft zijn de leden van de PVV-fractie bezorgd over meer internet governance.

Tot slot willen de leden van de PVV-fractie de diplomaten die zich met deze taaie materie bezighouden, sterkte wensen. De ontwikkelingen in het cyberdomein gaan snel en de omstandigheden zijn uitdagend. Deze leden hopen desondanks dat er voor Nederland toch positieve resultaten geboekt worden de komende periode.

Vragen en opmerkingen van de leden van de GroenLinks-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de brief over de voortgang van de Internationale Cyberstrategie en hebben daarover de volgende vragen en opmerkingen.
Deze leden dringen aan op een solide internationale cyberstrategie in deze veranderende wereldorde. Digitalisering is verworden tot zowel het strijdtoneel als een wapen in het digitale tijdperk. Wij moeten de binnenlandse expertise volop inzetten en leidend zijn op dit vlak. Aan de hand van de drie doelstellingen van de strategie zullen deze leden hun opmerkingen en vragen uiteenzetten.

Doelstelling 1 – tegengaan van cyberdreigingen van staten en criminelen
De leden van de GroenLinks-PvdA-fractie hebben grote zorgen over de aanhoudende cyberdreigingen gericht op Nederland en de rest van Europa. Er woedt een cyberoorlog achter de schermen, waarvan de schaal en ernst lastig te bevatten zijn. Het is van onmiskenbaar belang dat Nederland beschikt over betrouwbare inlichtingen en snel kan opereren.

Kan de minister meer vertellen over de intensievere informatie-uitwisseling tussen de betrokken ministeries, de inlichtingen- en veiligheidsdiensten, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), Nationaal Cyber Security Centrum (NCSC), politie en het Openbaar Ministerie (OM)? Welke ministeries zijn er betrokken bij deze uitwisseling en wat is precies hun rol?

6. Antwoord van het kabinet

Bij het cyberveilig houden van Nederland is een groot aantal ministeries en uitvoeringsinstanties betrokken. Effectieve informatie-uitwisseling is daarom cruciaal. Doelstelling van die informatie-uitwisseling is om het effect van responsmaatregelen in reactie op cyberdreigingen zo groot mogelijk te maken. Deze responsmaatregelen kunnen zowel gericht zijn op het versterken van de nationale cyberweerbaarheid als op het ontmoedigen van kwaadwillende actoren (bijvoorbeeld via attributieve verklaringen of sancties). Informatie over cyberdreigingen wordt gedeeld tussen het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het ministerie van Defensie, het ministerie van Justitie en Veiligheid (inclusief NCTV) en ministerie van Buitenlandse Zaken. Ook de AIVD, MIVD, het NCSC, Politie en OM zijn nauw bij deze inzet betrokken. De genoemde organisaties leveren elk informatie op basis van hun eigen mandaat.

Hoe wil de minister bestaande samenwerkingen, ook de publiek-private samenwerking tussen internationale / Europese cybersecuritybedrijven en overheden, verdiepen? Is de samenwerking met internationale partners naar wens vastgelegd in onze nationale wetgeving?

7. Antwoord van het kabinet

Publiek-private samenwerking, zowel binnen Nederland als internationaal, is essentieel bij het vergroten van de nationale weerbaarheid tegen cyberdreigingen. De dreigingsinformatie waar private partijen over beschikken vormen vaak een relevante aanvulling op de dreigingsinformatie van overheden. Op nationaal niveau zijn de afgelopen jaren door middel van het platform Cyclotron concrete stappen gezet op het gebied van institutionalisering van de samenwerking tussen overheden en bedrijven bij het tegengaan en mitigeren van cyberdreigingen. Voor meer informatie over Cyclotron verwijs ik graag naar het antwoord op vraag 13.

Bij de bevordering van internationale publiek-private samenwerking speelt Nederlands Cybersecurity Coördinatiecentrum (NCC NL) een belangrijke rol. NCC-NL verbindt de Nederlandse cybersecuritygemeenschap aan Europese partijen voor gezamenlijke inschrijving op EU-subsidietrajecten, zowel door subsidiemogelijkheden onder de aandacht te brengen als door bij te dragen aan consortiumvorming.

De leden van de GroenLinks-PvdA-fractie hebben nog altijd grote bedenkingen bij de Tijdelijke Wet Cyberoperaties, die de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) uitbreidt. Zij vinden het onnavolgbaar dat er een wet in werking is getreden, waarvan zowel de toezichthouder als de inlichtingendiensten erkennen dat deze onuitvoerbaar is door het ontbreken van adequaat toezicht. Door huisvestingsproblematiek voort te laten duren, heeft het kabinet het onmogelijk gemaakt voor de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) om op volle kracht te komen en haar taken uit te voeren.

Wat is volgens de minister het gevolg van deze situatie voor de nationale veiligheid? Wat doet het voortduren van deze situatie met het internationale aanzien van de Nederlandse inlichtingen- en veiligheidsdiensten? Hoe lang duurt het, totdat er is voldaan aan de randvoorwaarden van de Tijdelijke Wet Cyberoperaties en de CTIVD daadwerkelijk uitvoering kan geven aan haar toezichtstaken? Hoe zorgt de minister ervoor dat de CTIVD volledig is uitgerust en op volle kracht is, voordat de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) de nieuwe bevoegdheden inzetten? In welke opzichten kan Nederland leren van toezichtregimes op diensten van bondgenoten? Is de minister bereid lessen te trekken uit hun werkwijzen en deze te betrekken bij de herziening van de Wiv 2017? Welke landen zijn wat de minister betreft toonaangevend op het gebied van hun inlichtingen- en veiligheidsdiensten en het bijbehorende toezicht?

8. Antwoord van het kabinet

De verhuizing van de CTIVD is inmiddels afgerond en de personeelswerving is geïntensiveerd. Hierdoor kunnen de toezichthouder en de diensten hun samenwerking intensiveren en streven ze naar een volledige toepassing van de Tijdelijke Wet Cyberoperaties op de kortst mogelijke termijn. De wet, die per 1 juli 2024 in werking is getreden, is essentieel voor de nationale veiligheid, gezien de geopolitieke situatie en de noodzaak om snel te reageren op landen met een offensief cyberprogramma, zoals China en Rusland. De wet wordt momenteel gedeeltelijk toegepast, met afspraken tussen de CTIVD en de diensten over de inzetbare bevoegdheden ondanks de personeelstekorten.

Wat betreft toezicht leert Nederland van de lessen van landen zoals Zweden, Denemarken, Frankrijk en het Verenigd Koninkrijk. In het kader van de herziening van de Wiv 2017 wordt een rechtsvergelijkend onderzoek uitgevoerd. De bevindingen uit dit onderzoek kunnen helpen bij de verdere verbetering van het toezichtstelsel, rekening houdend met de verschillen tussen de landen.

De leden van de GroenLinks-PvdA-fractie vragen om investeringen in de maatschappelijke weerbaarheid en digitale slagkracht. De acute dreigingen en de instabiele geopolitieke verhoudingen vragen om actie op het gebied van onze digitale veiligheid.

Het is echter niet meteen duidelijk wat de minister bedoelt met “maatschappelijke weerbaarheid” en “digitale slagkracht,”; dit zijn namelijk brede termen. Hoe definieert de minister deze termen?

9. Antwoord van het kabinet

Zoals uiteengezet in de Kamerbrief van 6 december jl. ziet het kabinet een weerbare maatschappij als een maatschappij die schokken aankan, ongeacht wat er op ons afkomt.[6] Het is een maatschappij waarin overheid, publieke en private partners, maatschappelijke organisaties, kennisinstellingen en inwoners zoveel mogelijk voorbereid zijn op maatschappelijke ontwrichting en het vermogen hebben deze te weerstaan, op te vangen en ervan te herstellen. Niet alleen bij hybride aanvallen of een militair conflict, maar ook bij andere crises, zoals grootschalige overstromingen, een pandemie of langdurige uitval van vitale processen.

[6] Kamerbrief over weerbaarheid tegen militaire en hybride dreigingen, Kamerstuk 30821, nr. 249

Maatschappelijke weerbaarheid en militaire paraatheid zijn de pijlers van de weerbaarheidsopgave. Concreet vereist maatschappelijke weerbaarheid bescherming van vitale en andere belangrijke processen, een parate en veerkrachtige samenleving, het overeind houden van de Nederlandse democratie, rechtstaat en overheid en een weerbare economie. Dit gebeurt met name door het implementeren van de Europese NIS2-richtlijn in de Cyberbeveiligingswet en het uitvoeren van de Nederlandse Cybersecurity Strategie. Hiermee maken we Nederland digitaal weerbaar in een situatie van toenemende hybride en militaire dreiging.

Digitale slagkracht betreft de capaciteit van Nederland om zelf effectief te kunnen optreden in het digitale domein. Belangrijkste spelers hierin zijn de krijgsmacht, de MIVD, de AIVD en het Nationaal Cyber Security Centrum, met ieder hun eigen taak. Digitale slagkracht richt zich o.a. op het kunnen onderkennen en verstoren van cyberdreigingen, het uitvoeren van (militaire) cyberoperaties die zowel defensief als offensief van aard kunnen zijn, het op verzoek ondersteuning leveren aan bondgenoten bij de detectie van en reactie op kwaadwillende cyberoperaties en het adequaat reageren op digitale dreigingen en incidenten bij Nederlandse publieke en private organisaties.

Kan hij toelichten welke "investeringen in de digitale slagkracht" van het Ministerie van Defensie hij precies bedoelt? Hoeveel middelen zijn er precies geïnvesteerd en welk doel dienden deze investering? Kan de minister aantonen dat deze investeringen hebben bijgedragen aan onze digitale slagkracht?

10. Antwoord van het kabinet

De investeringen in de digitale slagkracht van Defensie richten zich op het versterken van de militaire cybercapaciteit, met name het vergroten van het aantal teams voor militaire cyberoperaties en het vergroten van cyberkennis binnen de krijgsmacht. Deze investeringen volgen uit de Defensienota's 2022 en 2024. Defensie investeert continu in innovatieve militaire cybertoepassingen, samen met academici, bedrijven en andere overheden.

Enkele concrete investeringen zijn: de versterking van militaire cybercapaciteiten van het Defensie Cyber Commando (DCC) en het versterken van de kennisfunctie bij *Cyber Warfare & Training Centre* (CWTC) van het DCC. Buiten het DCC investeren ook de Defensie Onderdelen in de digitale slagkracht met het oogmerk om operationele en tactische effecten te kunnen sorteren indien de omstandigheden daarom vragen en indien daar een wettelijke grondslag voor bestaat.

De leden van de GroenLinks-PvdA-fractie lezen met interesse over de offensieve capaciteiten van de MIVD, naast de defensieve capaciteiten.

Kan de minister in algemene zin iets zeggen over de offensieve cyberstrategie van Nederland? Wat zijn de bijzondere capaciteiten van Nederland en hoe zetten wij deze in om bondgenoten te ondersteunen? Is het wel of niet ondersteunen van bepaalde bondgenoten in offensieve operaties een diplomatieke afweging en, zo ja, hoe bepaalt het kabinet wanneer Nederland te hulp schiet?

11. Antwoord van het kabinet

Nederland heeft een Defensie Cyber Strategie. Deze ondergaat momenteel een herziening waarmee het kabinet beoogt bestaande instrumenten proactiever in te kunnen zetten om weerstand te bieden tegen de aanhoudende cyberdreiging.

In de eerste plaats gaat het daarbij om de inlichtingen- en contra-inlichtingencapaciteiten van de AIVD en MIVD. In aanvulling daarop voert Defensie met militaire cybercapaciteiten (defensieve) cyberoperaties uit, met als doel bondgenoten te ondersteunen en agressieve cyberactoren tijdig te onderkennen. Deze operaties worden uitgevoerd binnen de kaders van nationaal en internationaal recht, en kunnen pas plaatsvinden na een regeringsbesluit.

Defensie zet militaire cybercapaciteiten in voor zowel offensieve als defensieve operaties. Defensieve operaties richten zich op het neutraliseren van aanvallen en het behouden van vrijheid van handelen. Offensieve cyberoperaties kunnen bijvoorbeeld systemen uitschakelen, de beschikbaarheid ervan ontzeggen, of data (onopgemerkt) manipuleren. De inzet van militaire cybercapaciteiten, voor offensieve operaties, is net als de inzet van de rest van de krijgsmacht gebonden door het (inter)nationaal recht en geschiedt alleen na besluit van de regering tot inzet.

Diplomatieke afwegingen kunnen een rol spelen bij het besluit om bondgenoten te ondersteunen met militaire cyberoperaties, waarbij de regering kijkt naar de noodzaak, het mandaat en de internationale context. Hierin worden altijd internationaalrechtelijke principes gevolgd.

Wanneer verwacht de minister uitkomsten van het Defensieonderzoek over een mogelijke wettelijke grondslag voor “de digitale bescherming van onze samenleving”? Welke acties schaart hij onder deze bescherming?

12. Antwoord van het kabinet

Om effectief op te treden in het digitale domein, benut Defensie de ruimte binnen de bestaande juridische kaders. Waar is vastgesteld dat bestaande juridische kaders knellen, wordt aanpassing van bestaande en ontwerp van nieuwe wetgeving overwogen en/of in gang gezet. In deze context heeft het onderzoek naar de mogelijkheden voor een wettelijke grondslag in ‘een Wet op de gereedstelling’, zoals genoemd in Kamerstukken II 2024/25, 33 321, nr. 10, inmiddels geresulteerd in de voorbereiding van een wetsvoorstel voor de Wet op de Defensiegereedheid. Beoogd wordt om dit wetsvoorstel op korte termijn in consultatie te brengen.
Defensie ondersteunt de cyberweerbaarheid van de samenleving door informatie en inlichtingen te delen, met prioriteit voor kritieke overheidsfuncties en vitale processen. Defensie draagt bij aan de cyberverdediging van Nederland en bondgenoten via defensieve cyberoperaties en ondersteunt civiele overheden en private partners in capaciteitsopbouw, handhaving, detectie en respons.

Vanuit de inlichtingen- en veiligheidstaak van de MIVD onderkent Defensie cyberdreigingen door tegenmaatregelen te nemen en handelingsopties van kwaadwillende

actoren te beperken. Ook de marechaussee draagt binnen haar taakstelling met unieke opsporingsbevoegdheden bij aan een veilige samenleving door de digitale bestrijding van (gedigitaliseerde) criminaliteit. Ter versterking van de cyberweerbaarheid van defensie maar ook de samenleving, is goede *Cyber Threat Intelligence* (CTI) essentieel. Hiervoor is het noodzakelijk dat wettelijke kaders verruimd worden om defensie in staat te stellen om op proportionele en subsidiaire wijze intelligence te verzamelen die noodzakelijk is voor onze weerbaarheid.

Deze leden pleiten verder voor een vorm van 'samenredzaamheid' om in het geval van een langdurige cyberaanval of stroomstoring de samenleving draaiende te houden. Dat gaat verder dan het individuele belang om een noodpakket in huis te hebben en vraagt om een wijkbrede aanpak. Hierbij kijken deze leden met interesse naar de aanbevelingen van het rapport van de Adviesraad Internationale Vraagstukken (AIV) "Hybride dreigingen en maatschappelijke weerbaarheid" van juni 2024.[7]

Maatschappelijke weerbaarheid is altijd collectief, niet individueel. Hoe ziet de minister een collectieve aanpak voor maatschappelijke weerbaarheid voor zich? Wat vraagt dit van individuen, overheden en bedrijven?

13. Antwoord van het kabinet

Veiligheid is een kerntaak van de overheid, maar de overheid kan het niet alleen. Betrokkenheid van de hele samenleving is essentieel in het versterken van de weerbaarheid tegen hybride en militaire dreigingen: overheid, bedrijfsleven, maatschappelijke organisaties, kennisinstellingen en burgers. Samen moeten we de gevolgen van een conflict zo goed mogelijk op kunnen vangen en onder buitengewone omstandigheden kunnen blijven functioneren.

Dit vraagt van burgers bijvoorbeeld dat zij voorbereid zijn op situaties van langdurige uitval en daar de nodige voorbereidingen voor treft zodat je de eerste 72 uur doorkomt als hulp langer op zich laat wachten. Het bedrijfsleven is een belangrijke speler in het waarborgen van de continuïteit van onze maatschappij, zoals vitale processen als energie en communicatie en het voorzien in primaire levensbehoeften zoals voedsel. Op het gebied van cyber intensiveren we de publiek-private samenwerking en informatie-uitwisseling over cyberdreigingen met het programma Cyclotron en bouwen we verder aan het cyberweerbaarheidsnetwerk. In dit netwerk komen publieke en private organisaties samen om te werken aan cyberweerbaarheid van de eigen organisatie en van alle organisaties die zij vertegenwoordigen. Ook zullen bepaalde sectoren of bedrijven voorbereid moeten zijn op het ondersteunen van de inzet van onze krijgsmacht. Voor gemeenten en veiligheidsregio's ligt er een belangrijke rol om de kracht van burgers en organisaties te verbinden aan de weerbaarheidsopgave.

Het maatschappij brede gesprek hierover wordt intensief gevoerd via bestaande netwerken en aanvullende initiatieven, zoals het inrichten van een publiek-private geopolitiek en weerbaarheidsberaad.

[7] Hybride dreigingen en maatschappelijke weerbaarheid | Publicatie | Adviesraad Internationale Vraagstukken (juni 2024)

Hoe kijkt de minister naar de Finse maatregel om per 2028 300 crisisbestendige winkels te openen, die in het geval van een nationale crisis essentiële goederen kunnen blijven leveren?[8] Kan de minister een uitgebreide reflectie geven op de toepasbaarheid van deze maatregel voor Nederland?

14. Antwoord van het kabinet

Het kabinet heeft gekeken naar ervaringen van andere landen op het gebied van versterking van de weerbaarheid, specifiek naar Oekraïne, Finland, Zweden en het VK. Mede onder onze leiding bouwen we aan een coalitie met Zweden, Finland, Estland, Letland, Litouwen, België, Luxemburg en het VK. Met deze landen wisselen we continue ervaringen uit. Daarnaast wordt ook in EU-verband ingezet op de uitwisseling van ervaringen en *best practices*.

Het kabinet is zich bewust van het belang van continuïteit van de samenleving in een crisissituatie. Het is essentieel dat burgers goed voorbereid zijn op zo'n crisis, onder meer met een noodpakket met essentiële goederen waarmee je 72 uur vooruit kunt mocht hulp langer op zich laten wachten.

De aanpakken van andere landen zijn echter niet één op één over te nemen. Veelal verschilt de veiligheidscultuur, dreigingscontext en (beleids)geschiedenis. Om die reden zullen we zoeken naar een Nederlands antwoord en zullen de ervaringen vertaald moeten worden naar de Nederlandse context. Dit geldt ook voor de Finse maatregel van crisisbestendige winkels. Verdeling van schaarste en het vraagstuk van distributie in crisissituaties heeft onze nadrukkelijke aandacht. Voor het zomerreces wordt uw Kamer nader geïnformeerd over de concrete beleidsinzet ten aanzien van de weerbaarheidsopgave.

De leden van de GroenLinks-PvdA-fractie zijn benieuwd hoe de minister kijkt naar de relatie met de VS op het gebied van inlichtingen delen, gezien de recente geopolitieke ontwikkelingen. De VS heeft besloten Rusland niet meer als tegenstander te beschouwen op het gebied van cyberaanvallen, terwijl dit een land is waarvan wij weten dat het cyberoperaties uitvoert om Europa te ondermijnen. Het gevolg hiervan is logischerwijs dat Rusland cyberoperaties die eerst gericht waren op de VS, nu op de Europese Unie (EU) zal richten.

Wat betekent de draai van de VS voor de betrouwbare informatie-uitwisseling met de Amerikaanse inlichtingendiensten? Heeft de minister de AIVD en de MIVD geraadpleegd over hun zienswijze op de nieuwe positie van de VS en welke consequenties Nederland daaraan moet verbinden? Wat is het huidige Amerikastandpunt van dit kabinet en zijn de recente ontwikkelingen mogelijk aanleiding om deze te herzien en bepaalde informatie niet meer met de VS uit te wisselen? Hoe gaan andere bondgenoten hiermee om?

15. Antwoord van het kabinet

De berichten dat de VS zijn beleid ten aanzien van de Russische cyberdreiging zou aanpassen zijn onbevestigd. De VS zijn altijd een belangrijke partner geweest bij het

[8] 300 crisis-situation food stores to open « Euro Weekly News (16 maart 2025)

tegengaan van statelijke cyberdreigingen, zowel op het gebied het uitwisselen van inlichtingen als op diplomatieke inzet. Het kabinet zet erop in die relatie waar mogelijk voort te zetten.

De minister van Defensie heeft de AIVD en MIVD geraadpleegd over de recente ontwikkelingen, maar doet geen uitspraken over de bilaterale relatie met de Amerikaanse inlichtingendiensten. De opstelling van de VS heeft geen directe gevolgen voor de informatie-uitwisseling, aangezien Nederland zijn afwegingen blijft maken op basis van de nationale veiligheid en de internationale context. Het kabinet blijft de situatie monitoren en stelt geen wijzigingen in de informatie-uitwisseling met de VS voor op dit moment. Andere bondgenoten maken hun eigen afwegingen, die afhankelijk zijn van hun nationale belangen en samenwerkingsverbanden.

In hoeverre zijn onze inlichtingen- en veiligheidsdiensten afhankelijk van Amerikaanse informatie, maar ook van Amerikaanse techleveranciers voor de eigen ICT-huishouding?

16. Antwoord van het kabinet

Internationale samenwerking, waaronder met de VS, is essentieel voor de nationale en internationale veiligheid. De AIVD en MIVD werken regelmatig samen met internationale partners, maar geven geen details over specifieke samenwerkingsverbanden of gegevensuitwisseling. Bij het uitvoeren van hun werk wegen de diensten alle relevante omstandigheden mee.

Wat betreft de ICT-huishouding, werken de diensten samen met verschillende leveranciers, waaronder Amerikaanse bedrijven. Er wordt momenteel gekeken naar het gebruik van Amerikaanse producten en de wenselijkheid hiervan.

Is het terugdringen van strategische afhankelijkheden op het gebied van inlichtingen en de eigen ICT een onderdeel van de Internationale Cyberstrategie? Zo ja, welke middelen heeft de minister hiervoor beschikbaar?

17. Antwoord van het kabinet

Het vraagstuk van strategische afhankelijkheden op het gebied van inlichtingen en ICT vallen buiten de scope van de Internationale Cyberstrategie.

De leden van de GroenLinks-PvdA-fractie uiten ook hun zorgen over de steun voor initiatieven die te maken hebben met Starlink. De belangen van de eigenaar van Starlink, die als rijkste man ter wereld een prominente positie heeft veroverd in het hart van de macht in de regering-Trump, kunnen haaks staan op Nederlandse en Europese belangen. Sowieso hebben de leden zorgen over de vermenging van economische en politieke belangen tussen de Amerikaanse regering en Starlink.

Zijn de recente ontwikkelingen in de VS aanleiding voor de minister om de inzet en financiering van Starlink-satellieten te heroverwegen? Hoe kijkt de minister naar de stukgelopen

onderhandelingen tussen Italië en Starlink?[9] Is dit volgens hem een waarschuwing dat een eenzijdige afhankelijkheid van Starlink een strategisch risico is? Op welke manier kunnen Europese lidstaten en andere bondgenoten deze afhankelijkheid voorkomen? Is het denkbaar dat Europa investeert in een eigen satellietennetwerk?

18. Antwoord van het kabinet

Het kabinet heeft geen zicht op de onderhandelingen tussen Italië en Starlink. Wel onderkent het kabinet het belang van diversificatie in het afnemen van diensten van aanbieders van satellietcommunicatie.

Europa werkt actief aan versterking van de strategische autonomie op dit terrein. De Europese Commissie ontwikkelt in dat kader het programma IRIS²: een Europese satellietconstellatie van circa 300 satellieten in verschillende banen om veilige, robuuste en wereldwijde communicatie mogelijk te maken. Het systeem is bedoeld als aanvulling op bestaande netwerken en kan dienen als terugval infrastructuur voor publieke telecommunicatie bij uitval of crises. Dit wordt verkend in het kader van bijvoorbeeld hybride of militaire dreigingen. In de Lange-termijn Ruimtevaartagenda, die in februari aan de Kamer is gestuurd, bent u hierover geïnformeerd. De IRIS²-wetgeving bevat bovendien bepalingen die zorgen voor deelname van het midden- en kleinbedrijf aan aanbestedingen, wat past bij het Nederlandse belang van diverse industriële toegang. Nederland ondersteunt de ontwikkeling van IRIS² en zet, binnen de beschikbare middelen, in op gerichte deelname van Nederlandse partijen aan dit strategisch belangrijke Europese project. Tegelijk blijft internationale samenwerking – o.a. binnen NAVO-verband – van belang voor interoperabiliteit en toegang tot kritieke infrastructuur in de ruimte.

Tot slot op deze doelstelling zijn de leden van de GroenLinks-PvdA-fractie benieuwd naar de inzet op verantwoordelijk statelijk gedrag in het cyberdomein. Deze leden steunen de proactieve inzet van het kabinet op dit gebied en vinden het passen bij Nederland dat zij de gezamenlijke waarden bewaart en bewaakt.
Echter vragen deze leden om een duidelijke definitie van “verantwoordelijk statelijk gedrag en de toepassing van internationaal recht in het cyberdomein.” Kan de minister op een begrijpelijke manier uitleggen wat dit betekent en waarom dit nodig is? Wat bedoelt hij precies met het “hoger op de agenda van de VN krijgen” van bepaalde onderwerpen? Kan hij concreet maken wat de Nederlandse inzet hierin heeft opgeleverd?

19. Antwoord van het kabinet

Het kabinet hecht ook in het cyberdomein sterk aan de internationale rechtsorde. Staten dienen zich te richten naar internationale normen die in VN-kader zijn afgesproken. Hoewel niet bindend, zijn deze normen richtinggevend voor gedrag van staten binnen het cyberdomein. Het normatief kader vormt het uitgangspunt om landen aan te kunnen spreken en verantwoordelijk te houden in geval van schendingen.
Binnen de VN-werkgroep die zich met cybervraagstukken bezighoudt wordt over een breed scala aan onderwerpen gesproken, onder andere over de erkenning van de meest stringente dreigingen in het cyberdomein waar landen mee geconfronteerd worden. In dit

[9] Onderhandelingen tussen Italiaanse regering en Starlink zijn vastgelopen - IT Pro - Nieuws - Tweakers

kader heeft Nederland de dreiging die uitgaat van *ransomware*-aanvallen op de agenda gekregen alsook dat landen zich moeten weerhouden van aanvallen op internationale organisaties, volgend op de omvangrijke cyberaanvallen op het International Strafhof in september 2023. Door inzet van Nederland zijn deze dreigingen vastgelegd in het jaarrapport van de werkgroep.

Doelstelling 2 – versterken van democratische en mensenrechtelijke principes online
De leden van de GroenLinks-PvdA-fractie roepen de minister op om zich blijvend als aanjager van waarden gedreven digitalisering in te zetten. Het digitale tijdperk brengt nieuwe uitdagingen met zich, met name op het gebied van privacy en veiligheid.

Welke waarden, principes en rechten zijn volgens de minister leidend in het digitale domein? Kan hij uitgebreider toelichten op welke vlakken deze democratische en mensenrechtelijke principes momenteel onvoldoende geborgd zijn online?

20. Antwoord van het kabinet
Nederland streeft naar een open, vrij en veilig cyberdomein. Toepassing van het internationaal recht, inclusief mensenrechten, is hierin leidend voor het kabinet. Ook streeft het kabinet democratische waarden en naleving van de principes van de rechtstaat na in het digitale domein.

Mensenrechten en democratische waarden zijn online op meerdere vlakken onvoldoende geborgd. Zo staat het recht op privacy onder druk door grootschalige digitale surveillance door zowel overheden als bedrijven. In het bijzonder voor journalisten en mensenrechtenverdedigers is dit schadelijk vanwege hun rol in het bevorderen en beschermen van mensenrechten. Vrijheid van meningsuiting wordt ingeperkt door *internet shutdowns*, blokkades, censuur en disproportionele straffen voor online uitingen in autoritaire regimes. Daarnaast ondermijnen (statelijke) desinformatiecampagnes — vaak verspreid via sociale media en soms door algoritmes versterkt — het open democratisch debat. Desinformatie heeft impact op het recht op toegang tot pluriforme, betrouwbare informatie, tast het vertrouwen in instituties aan en verzwakt de weerbaarheid van samenlevingen.

Het gebrek aan transparantie in algoritmes en moderatieprocessen bij grote technologiebedrijven heeft directe gevolgen voor de publieke opinievorming. Dit probleem wordt binnen de Europese Unie inmiddels geadresseerd door de digitaledienstenverordening (*Digital Services Act*, "DSA"), op grond waarvan (zeer grote online) platforms onder meer transparant moeten zijn over hun aanbevelingssystemen (en de parameters daarvoor) en moderatieprocessen. Daardoor krijgen gebruikers meer inzicht in welke informatie zij te zien krijgen en waarom. Ook geeft de DSA gebruikers verschillende mogelijkheden om moderatiebeslissingen van online platforms aan te vechten.

Wat heeft de minister concreet voor elkaar gekregen in de brede coalitie met landen, bedrijven en experts om betere bescherming af te dwingen?

21. Antwoord van het kabinet

Regulering en bescherming van fundamentele rechten online verloopt binnen Nederland primair via EU-wetgeving, zoals de DSA. Tegelijkertijd is internationale normstelling essentieel, vanwege het grensoverschrijdende karakter van het digitale domein. Juist nu het multilaterale systeem onder druk staat, is het van groot belang om via coalities als de *Freedom Online Coalition* (FOC) een krachtig democratisch tegenwicht te bieden aan autoritaire invloeden binnen de VN en andere internationale fora.

Het afgelopen jaar (2024) was Nederland voorzitter van de FOC. Als voorzitter heeft Nederland de volgende concrete stappen gezet om digitale rechten wereldwijd te verdedigen:

1. **Waarden en principes verankerd in de *VN Pact for the Future*, inclusief de *Global Digital Compact,* en de eerste AVVN-resolutie over AI. Daarmee biedt het tegenwicht aan autoritaire invloeden binnen de VN. In dat forum heeft de *FOC* het belang van het *multistakeholder*-model en de bescherming van mensenrechten online krachtig verdedigd tegen autoritaire pogingen tot meer staatscontrole over het internet.**
2. **De publicatie van de *'Joint Statement on Technical Standards and Human Rights in the Context of Digital Technologies'*: in deze verklaring benadrukt de FOC het belang van het integreren van mensenrechten in de ontwikkeling van technische standaarden voor digitale technologieën. Naast alle FOC landen, is deze gezamenlijke verklaring ook getekend door Cyprus, Griekenland, Malta, Portugal en Roemenië.**
3. **In samenwerking met Denemarken en de Wikimedia Foundation heeft Nederland de *'Blueprint on Information Integrity'* gelanceerd; de *blueprint* stelt hoe het online informatielandschap ingezet kan worden ter bevordering van vrijheid van meningsuiting en toegang tot informatie (met name in de periode rondom verkiezingen), gebaseerd op de principes van *'Agency', 'Trust'* en *'Inclusion'*.**
4. **Tijdens het Nederlands voorzitterschap zijn Kaapverdië, Slovenië, Colombia en Armenië toegetreden tot de FOC, waardoor het aantal leden is gegroeid tot 42.**

De leden van de GroenLinks-PvdA-fractie zien een gouden rol weggelegd voor Nederland in het vechten voor een democratisch en veilig internet. Al decennia is Nederland een pionier op het gebied van de online wereld, met toonaangevende ICT'ers en denkers die hebben bijgedragen aan zowel de theoretische als praktische basis voor het moderne internet.

Hoe benut de minister de Nederlandse expertise in de Internationale Cyberstrategie? Doet hij een beroep op alle kennis die wij als land in huis hebben, ook buiten de overheid om, om bij te dragen aan een veiliger internet? Hoe betrekt de minister zijn collega's van Binnenlandse Zaken en Onderwijs, Cultuur en Wetenschap bij het bestrijden van statelijke desinformatie en het bevorderen van een vrij online medialandschap?

22. Antwoord van het kabinet

Bij het bestrijden van statelijke desinformatie en het bevorderen van een vrij online medialandschap doet Nederland veelvuldig beroep op kennis, en expertise van verschillende technisch experts, bedrijven en organisaties. Dit is een fundamenteel onderdeel van de uitvoering van de Internationale Cyberstrategie. De belanghebbende organisaties zijn zowel publiek als privaat; en zij komen samen in netwerkorganisaties. Zo

is het ministerie van Buitenlandse Zaken, evenals het ministerie van Economische Zaken, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het ministerie van Justitie en Veiligheid en het ministerie van Onderwijs, Cultuur en Wetenschappen, deelnemer van de netwerkorganisatie ECP | Platform voor de Informatiesamenleving. Met medewerking van ECP komen de betrokken ministeries tweejaarlijks bijeen met een brede groep Nederlandse stakeholders, waarin de uitvoering en voortgang van de Internationale Cyberstrategie tegen het licht wordt gehouden.

Daarnaast zijn het ministerie van Economische Zaken en het ministerie van Buitenlandse Zaken betrokken bij de organisatie door ECP van het jaarlijkse NLIGF (Nederlandse Internet Governance Forum) waarin we met o.a. academici, de technische gemeenschap, maatschappelijk middenveld en het bedrijfsleven diverse vraagstukken omtrent het beheer van het internet op nationaal niveau bespreken. Ook wordt er samengewerkt met kennisinstanties, zoals met de Universiteit Leiden in het *The Hague Program on International Cyber Security.*

Over hoe de verschillende ministers binnenlands samenwerken op het gebied van desinformatie is uw Kamer geïnformeerd in de Rijksbrede strategie voor effectieve aanpak van desinformatie en de daaropvolgende Voortgangsbrief.[10]

Welke nationale wetgeving kennen andere landen, die effectief is gebleken in het bestrijden van desinformatie?

23. Antwoord van het kabinet

Het kabinet verkent continu de internationale ontwikkelingen rondom desinformatie om effectieve interventies te formuleren. Zodoende wordt ook gekeken naar wetgeving in andere landen op dit gebied. De afgelopen jaren is er wereldwijd verschillende wetgeving verschenen met als doel desinformatie te bestrijden met zo min mogelijk inperking op fundamentele rechten, zoals het recht op vrijheid van meningsuiting. Voorbeelden hiervan zijn de Europese DSA en *de Online Safety Act* in het VK. Deze wetgeving is echter nog te kortgeleden geïntroduceerd om de effectiviteit in de bestrijding van desinformatie of de impact op mensenrechten te kunnen meten.

Ook zetten landen succesvol in op aanvullende detectie van desinformatie. EU-lidstaten, zoals bijvoorbeeld Zweden en Frankrijk, beschikken over de capaciteit om desinformatie afkomstig van buitenlandse statelijke en niet-statelijke actoren te detecteren en analyseren. De minister van BZK heeft technische ondersteuning (TSI) gevraagd bij de Europese Commissie voor een onderzoek naar de ervaringen van deze lidstaten. Die ervaringen willen we meenemen in de versterking van detectie van desinformatie in Nederland die afkomstig is van buitenlandse actoren.

Hoe zorgt de minister ervoor dat de vrijheid van meningsuiting en de vrije toegang tot informatie niet onevenredig wordt ingeperkt?

[10] Zie *Rijksbrede strategie effectieve aanpak van desinformatie, TK 2022–2023, 30 821, nr. 173. En Voortgangsbrief Rijksbrede strategie voor de effectieve aanpak van desinformatie en aankondiging nieuwe acties, TK 2023–2024, 30 821, nr. 230*

24. Antwoord van het kabinet

Door in te zetten op het promoten van informatie integriteit en door mensenrechten voldoende aandacht te geven bij de implementatie van de DSA, worden deze rechten beschermd en niet ingeperkt. Nederland spreekt zich uit, bijvoorbeeld via de *Universal Periodic Review*, wanneer in andere landen wetgeving wordt aangenomen die online vrijheden onevenredig inperkt onder het mom van het tegengaan van desinformatie.

Hiervoor verwijs ik u ook naar het antwoord op vraag 22.

Kan hij duidelijker uitleggen wat het doel is van de *Hub on Information Integrity* van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO)?

25. Antwoord van het kabinet

De *Hub on Information Integrity* is een samenwerkingsplatform van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) dat landen helpt in het bestendigen en promoten van informatie integriteit, waarmee ook misinformatie en desinformatie wordt tegengegaan. In december 2024 werd bijvoorbeeld de OESO *Recommendation on Information Integrity* aangenomen door de Raad van de OESO. Dit beleidsdocument is geschreven binnen de hub. Daarnaast dient de hub als platform waarbinnen landen kennis met elkaar kunnen delen.
Hiermee wordt concreet beleidsmatige invulling gegeven aan de *Global Declaration on Information Integrity Online,* die Nederland met Canada vorig jaar lanceerde.

De leden van de GroenLinks-PvdA-fractie steunen het breder bekend maken van de *Digital Services Act* (DSA) in internationaal verband. Zij vragen de minister om, gezien de ontwikkelingen bij verschillende sociale media platforms om de menselijke contentmoderatie af te schaffen, een actuele reflectie hierop te geven.

Is hij het met deze leden eens dat nationale moderatieteams nodig zijn om effectief te handhaven op illegale, schadelijke en onwenselijke content online? Wat is zijn mening over ‘community notes,’ de methodiek waar steeds meer sociale media hun moderatie op inrichten? Vindt hij dit een afzwakking of versterking van de aanpak van desinformatie op online platforms?

26. Antwoord van het kabinet

Het kabinet is voorstander van contentmoderatie als middel om desinformatie tegen te gaan, waar zoveel mogelijk Europese regelgeving gevolgd dient te worden. De DSA bevat verschillende verplichtingen over inhoudsmoderatie. Zo moeten aanbieders van alle tussenhandeldiensten een zorgvuldig beleid ten aanzien van inhoudsmoderatie opnemen in hun algemene voorwaarden en dat beleid ook toepassen in de praktijk. Het is in beginsel aan de platforms zelf om hier invulling aan te geven. Kennis over taal, cultuur en maatschappelijke context is van groot belang bij het modereren van content.

Voor effectieve moderatie zijn meer middelen nodig dan enkel mogelijk is via menselijke moderatie door alleen platforms. AI en ‘*community notes*’ kunnen daar een nuttige bijdrage aan leveren. *Community notes* zijn een vorm van gemeenschaps-gedreven moderatie, waarmee gebruikers extra informatie of context kunnen toevoegen aan een

geplaatst bericht. Deze extra informatie wordt niet direct zichtbaar voor iedereen die het bericht ziet, maar verschijnt pas voor iedereen wanneer gebruikers uit verschillende groepen het eens zijn over de waarde van de toegevoegde informatie. Veel '*notes'* zijn echter niet zichtbaar wanneer er te weinig stemmen voor zijn en er geen consensus over is gevormd. Effectieve moderatie vraagt waarschijnlijk om een combinatie van menselijke moderatie, *community notes*, en/of geautomatiseerde middelen.

De DSA verplicht platforms om transparantie te bieden over de moderatie die zij verrichten, en de wijze waarop. Zo moeten zij onder meer rapporteren over de moderatie die zij hebben verricht, de geautomatiseerde middelen die daarbij eventueel zijn toegepast, en maatregelen die zijn genomen om opleiding en bijstand te verstrekken aan personen die de moderatie verrichten. Zeer grote online platforms en zoekmachines moeten daarnaast rapporteren over de personele middelen die worden ingezet voor inhoudsmoderatie, uitgesplitst per officiële taal van de EU-lidstaten, en over de kwalificaties en taaldeskundigheid van deze moderatoren. Hiermee wordt transparant of, en zo ja welke, platforms menselijke contentmoderatie verminderen en welke middelen zij inzetten om te modereren. Uit deze rapportages zal ook moeten blijken hoe effectief de verschillende vormen van contentmoderatie, waaronder *community notes,* zijn in het tegengaan van illegale content en desinformatie.

De DSA verplicht zeer grote online platforms en zoekmachines om een systeemrisicoanalyse uit te voeren voordat zij veranderingen in de functionaliteit doorvoeren die waarschijnlijk kritieke gevolgen kunnen hebben op systeemrisico's. Aanpassingen van moderatiemethodiek kunnen daaronder vallen. De resultaten van deze risicoanalyses moeten worden gedeeld met de Europese Commissie, die primair toeziet op naleving van de DSA door deze diensten. Dit stelt de Commissie in staat om zo nodig te onderzoeken welke gevolgen dit soort wijzigingen hebben op de systeemrisico's waarop het van invloed kan zijn. Indien zo'n wijziging leidt tot systeemrisico's dan heeft de Europese Commissie bevoegdheden om daar tegenop te treden.

De leden van de GroenLinks-PvdA-fractie zijn benieuwd naar samenwerking van de minister met de minister van Binnenlandse Zaken en de minister van Economische Zaken in het borgen van mensenrechten en democratische beginselen bij het ontwikkelen van standaarden voor opkomende technologieën.

Wat is hierin de rol van hun drie ministeries afzonderlijk?

27. Antwoord van het kabinet

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is het coördinerende departement op democratie, rechtsstaat en digitale zaken, waaronder de borging van grondrechten in de digitale wereld. Het ministerie houdt zicht op (nieuwe) digitale technologieën om kansen te omarmen en risico's voor mensenrechten en de democratie helder in beeld te hebben. Zo wordt er samen met TNO gewerkt om de impact van opkomende technologieën op publieke waarden in kaart te brengen. Daarnaast werkt het ministerie van BZK aan instrumenten voor verantwoorde digitalisering, zoals het Impact

Assessments voor Mensenrechten bij de inzet van Algoritmes (IAMA) en Kinderrechten Impact Assessments (KIA).

Het ministerie van Buitenlandse Zaken heeft het voorzitterschap van de *Freedom Online Coalition* in 2024 benut om het borgen van mensenrechten en democratische beginselen internationaal hoger op de internationale agenda te zetten, onder andere middels de door 41 landen onderschreven verklaring *Joint Statement on Technical Standards and Human Rights in the Context of Digital Technologies*[11]. Ook heeft Nederland met andere gelijkgezinde landen in 2024 in de VN gepleit voor het beschermen van mensenrechten in het digitale domein. Zo is een van de doelstellingen van het in 2024 aangenomen *UN Global Digital Compact* het promoten van een inclusieve, open, veilige en beveiligde digitale ruimte die mensenrechten respecteert, beschermt en bevordert. Ook worden standaardisatieorganisaties opgeroepen om de ontwikkeling te bevorderen van standaarden voor kunstmatige intelligentie die interoperabel, veilig, betrouwbaar en duurzaam zijn en mensenrechten borgen.

De ministeries van Economische Zaken en Buitenlandse Zaken zetten in de Internationale Telecommunicatie Unie (ITU) in op het ontwikkelen van een methode om de impact van technische standaarden op mensenrechten te kunnen evalueren.

Welke mensenrechten en democratische beginselen moeten volgens de minister beter geborgd worden in de standaarden voor nieuwe technologieën? Welke concrete resultaten, naast het ondertekenen van een gezamenlijk statement, heeft de minister hierin geboekt?

28. Antwoord van het kabinet

Technische standaarden voor het internet en digitale technologieën vervullen een essentiële rol in de wereldwijde interoperabiliteit, veiligheid en betrouwbaarheid van digitale technologieën. In die zin kunnen technische standaarden ertoe bijdragen dat digitale technologieën de uitoefening van mensenrechten versterken, zoals vrije toegang tot informatie en ideeën, vrijheid van meningsuiting, vrijheid van vergadering en privacy. Wanneer mensenrechten onvoldoende geborgd zijn in technische standaarden, kan de toepassing van technische standaarden leiden tot mensenrechtenschendingen, zoals massa surveillance, afgezwakte encryptiestandaarden, censuur, manipulatie van online verkeer en permanente identificatie van online gebruikers.
De ministeries van Binnenlandse Zaken, Economische Zaken en Justitie en Veiligheid werken samen bij het ontwikkelen van internationale en Europese AI-standaarden binnen het *Comité Européen de Normalisation / Comité Européen de Normalisation Electrotechnique* (CEN/CENELEC) en de *International Organization for Standardization/ International Electrotechnical Commission* (ISO/IEC); zo draagt Economische Zaken (financieel) bij aan de deelname van Nederlandse belanghebbenden en de bezetting van strategische functies in deze organisaties voor AI en cybersecurity. Door deelname aan de NEN-normcommissie '*AI* en *Big Data*', zetten ze in op de bescherming van fundamentele rechten binnen de

[11] Zie: Joint Statement on Technical Standards and Human Rights in the Context of Digital Technologies: Joint Statement on Technical Standards and Human Rights in the Context of Digital Technologies

normen onder de Europese AI-verordening en het uitdragen van het Nederlands standpunt bij ISO.

Het ministerie van Buitenlandse Zaken ondersteunt middels een meerjarig programma concreet de deelname en betrokkenheid van maatschappelijk middenveldorganisaties uit het mondiale zuiden aan multilaterale processen rond digitale technologieën en *internet governance*. Nederland is in contact met verschillende standaard-ontwikkelingsorganisaties[12] om innovatieve manieren te vinden om dit thema structureel voor het voetlicht te brengen. Ook op EU-niveau vinden er conversaties plaats, specifiek in het kader van de ontwikkeling van standaarden ten behoeve van de Europese *AI Act*. Het integreren van mensenrechten-overwegingen in de ontwikkeling van technische standaarden is een proces van de lange adem, maar er is groeiend momentum bij zowel standaard-ontwikkelingsorganisaties zelf als bij deelnemende belanghebbenden om voortgang te boeken op dit thema. Zo vond recentelijk een internationale conferentie plaats over AI-standaarden in Londen, mede georganiseerd door de *AI Standards Hub* van het *Alan Turing Institute*, de OESO en het VN Bureau van de Hoge Commissaris voor de Mensenrechten.

De leden van de GroenLinks-PvdA-fractie juichen de positie van Nederland als toonaangevende speler op het gebied van ethische AI van harte toe.
Zij vragen de minister om een reflectie op de vraag hoe Nederland deze positie heeft verworven. Wat doet hij om dit succes voort te zetten en uit te breiden? Hoe zorgt de minister ervoor dat Nederland internationaal aan kop blijft? Welke middelen heeft dit kabinet beschikbaar om de ethische inzet van AI verder te stimuleren?

29. Antwoord van het kabinet

Nederland heeft zich de afgelopen jaren gepositioneerd als internationale voortrekker in het bevorderen van verantwoord AI-gebruik in militaire toepassingen. Een duidelijk voorbeeld van de voortrekkersrol van Nederland op verantwoorde toepassing van AI in het militaire domein is het door Nederland gelanceerde REAIM-initiatief. Nederland heeft i.s.m. Zuid-Korea, Chili, Singapore, Turkije en Kenia verschillende mondiale en regionale bijeenkomsten georganiseerd om overheden, bedrijven, kennisinstellingen en het maatschappelijk middenveld bij elkaar te brengen om de dialoog over verantwoorde toepassing van AI in het militaire domein internationaal op de agenda te zetten en toe te werken naar concrete vervolgstappen. In het verlengde hiervan is met brede steun de Nederlandse VN resolutie over AI in het militaire domein afgelopen december aangenomen door de AVVN.

Breder gezien heeft Nederland deze positie opgebouwd door consistent in te zetten op een mensgerichte benadering van AI. De ontwikkeling van het Algoritmeregister en het Impact Assessment Mensenrechten en Algoritmes (IAMA), evenals versterkt toezicht dragen hier concreet aan bij. Ook speelt de Nederlandse kennisinfrastructuur een sleutelrol:

[12] Zoals de Institute of Electrical and Electronics Engineers (IEEE), de European Telecommunications and Standardisation Institute (ETSI), de Internet Engineering Task Force (IETF) en de Internationale Telecommunicatie Unie (ITU).

universiteiten en onderzoeksinstellingen leveren internationaal toonaangevend onderzoek op het gebied van verantwoorde AI.
Het kabinet zet deze inzet voort via gerichte investeringen, beleidsontwikkeling en internationale samenwerking. Nederland levert een actieve bijdrage aan multilaterale processen, waaronder in EU-verband en bij de VN, UNESCO en de Raad van Europa, om te komen tot gezamenlijke normen en standaarden voor betrouwbare en mensgerichte AI.

Gezien de taakstelling zijn de beschikbare middelen echter beperkt. Dit vraagt om scherpe prioritering, doelgerichte inzet en nauwe interdepartementale samenwerking en samenwerking met (inter)nationale partners. De komende AI-diplomatiestrategie zal deze inzet bundelen en voorzien van duidelijke richting.
Op welke manier ziet de minister voor zich dat internationaal recht en mensenrechten binnen de AI-strategie worden geborgd? Om welke internationale rechten en mensenrechten gaat het dan specifiek?

30. Antwoord van het kabinet
Nederland zet zich in voor erkenning dat het internationaal recht van toepassing is op het digitale domein, inclusief AI-toepassingen. Hierbij wordt specifiek aandacht besteed het humanitair oorlogsrecht en de mensenrechten, zoals het recht op privacy, verbod op discriminatie en de vrijheid van meningsuiting.
Uw Kamer zal in het najaar worden geïnformeerd over de geïntegreerde Nederlandse inzet op internationale AI-samenwerking op het gebied van veiligheid, internationaal recht en mensenrechten in een AI-diplomatiestrategie, die het ministerie van Buitenlandse Zaken ontwikkelt in samenwerking met de ministeries van Defensie, Justitie en Veiligheid, Binnenlandse zaken, Economische zaken en het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).[13]

Doelstelling 3 – behoud van een wereldwijd open, vrij en veilig internet
De leden van de GroenLinks-PvdA-fractie lezen met veel interesse over de inzet van de minister op een multistakeholder-model voor internetbeheer. Zij zijn het eens met het idee dat het internet, dat zo'n groot onderdeel van ons leven is geworden, om een democratische inrichting vraagt.

Deze leden zijn zeer benieuwd naar het toekomstbeeld van de minister van een meer democratisch internet. Wat vindt hij een gepast verdienmodel voor online diensten, die zich nu voordoen als 'gratis', maar eigenlijk massaal gebruikersdata doorverkopen? Welke verantwoordelijkheid hebben overheden en bedrijven in het beheren van het internet?

31. Antwoord van het kabinet
De overheid gaat niet over het verdienmodel van bedrijven, wel over de waarborgen die rechten van burgers beschermen. Het doorverkopen van gebruikersdata op zichzelf is niet verboden, mits aan de voorwaarden van de Algemene Verordening Gegevensbescherming (AVG) wordt voldaan. De AVG vereist voor iedere verwerking van persoonsgegevens een grondslag. Voor de doorverkoop van de hier bedoelde diensten is de grondslag die in aanmerking komt "toestemming" van betrokkene. Toestemming dient vrijelijk,

[13] Zie Motie Dijkstra CS, Voorgesteld tijdens het Notaoverleg van 22 april 2024, 26643-1151

ondubbelzinnig, geïnformeerd en specifiek te zijn gegeven en dient even gemakkelijk te kunnen worden ingetrokken. Verwerkingsverantwoordelijke online diensten moeten ervoor zorgen dat zij voldoen aan de wettelijke vereisten, en de naleving ervan te kunnen aantonen. Zij hebben een wettelijke verantwoordingsplicht.

Het toezicht op de AVG is belegd bij een onafhankelijke toezichthouder, in Nederland de Autoriteit Persoonsgegevens (AP). De toezichthouder beoordeelt per geval of een verwerking rechtmatig is. Omdat deze beoordeling niet alleen voorbehouden is aan de toezichthouder, maar bovendien bij uitstek afhankelijk van de feiten en omstandigheden, beperk ik mij tot deze algemene beantwoording.
De overheid stelt regels op, vaak in Europees verband. De AVG beschermt privacy online, en de digitale dienstenverordening (DSA) en marktverordening (DMA) bestrijden marktmacht, creëren toetredingsmogelijkheden voor alternatieven en concurrenten, en beschermen fundamentele rechten op grote platformen. Bedrijven moeten deze wetten naleven, door te werken aan een gezonde, veilige en betrouwbare online wereld.

De leden van de GroenLinks-PvdA-fractie onderschrijven de zorgen over een centraal en politiek aangestuurde inrichting van het internet. Bij voorkeur is het internet decentraal en federatief, opgebouwd uit aparte blokken, die ongevoelig zijn voor politieke inmenging. Ook hierin verzoeken deze leden met klem om de Nederlandse expertise volop te gebruiken.

Betrekt de minister bijvoorbeeld ook organisaties als Waag Futurelab en PublicSpaces bij het formuleren van zijn standpunt? Zo niet, is hij bereid dit alsnog te doen? Zo ja, op welke manier wordt hun expertise betrokken?

32. Antwoord van het kabinet
Ten behoeve van het formuleren van Nederlandse standpunten over het beheer van het internet worden veel verschillende stakeholders betrokken. Mede met dit doel is de Nederlandse overheid één van de stakeholders in het Nederlandse Internet Governance Forum (NLIGF), waarvoor de netwerkorganisatie ECP de coördinatie doet. Jaarlijks wordt er een NLIGF-bijeenkomst georganiseerd waarop actuele thema's worden geagendeerd. Waag Futurelab heeft bij het NLIGF in het verleden een *keynote* verzorgd. Daarnaast is in oktober 2024 een speciale gezamenlijke bijeenkomst georganiseerd door NLIGF, Internet Society Nederland en Platform Internet Standaarden. Zo is de betrokkenheid van Nederlandse stakeholders verbreed en zijn meer geïnteresseerden bereikt die mee kunnen en willen denken over het beheer van het internet. Alle geïnteresseerden zijn welkom om via deze weg aan te sluiten, zo ook de genoemde organisaties in de vraag.

Kan de minister de uitkomsten van de rondetafelbijeenkomst in oktober over internet governance aan de Kamer terugkoppelen?

33. Antwoord van het kabinet
In oktober 2024 hebben de ministeries van Economische Zaken en Buitenlandse Zaken een rondetafelbijeenkomst georganiseerd over internet fragmentatie, gefaciliteerd door ECP en met deelname van 14 experts vanuit verschillende stakeholder-groepen. Internet

fragmentatie is een gecompliceerd vraagstuk dat potentieel een weerslag heeft op verschillende lagen van het internet. Deelnemers deelden de inschatting dat een intentionele fragmentatie van de publieke kern van het internet (de vitale technische protocollen, standaarden en infrastructuren) onwaarschijnlijk is, omdat de economische voordelen van een wereldwijd interoperabel internet immers te groot zijn en is er wereldwijd een grote afhankelijkheid van het goed functioneren van het internet. Tegelijkertijd kan men op de laag van online content en applicaties al spreken van fragmentatie, door verschillende wet- en regelgeving rond digitale platformen en content.

De experts gaven aan dat het met name problematisch is als fragmentatie onbewust plaatsvindt als consequentie van (nationale) wet- en regelgeving over bijvoorbeeld cyberveiligheid, waardoor overheden een onevenredig grote rol innemen ten aanzien van *internet governance*.

Het kwantificeren van de economische waarde van een mondiaal opererend, decentraal georganiseerd open internet is echter een complexe exercitie, omdat het internet inmiddels in grote mate verweven is met de (online én offline) economie. Het blijkt ingewikkeld om de directe en indirecte financiële gevolgen van bijvoorbeeld beperkingen in e-mailverkeer tussen handelspartners te kwantificeren.

Naar aanleiding van deze rondetafelbijeenkomst wordt het in het internationale cyberstrategie aangekondigde onderzoek naar de economische consequenties van internet fragmentatie niet opportuun geacht en zal geen doorgang vinden. Het onderzoek wordt vanwege de vele variabelen en parameters te complex en zal waarschijnlijk geen concrete (nieuwe) conclusies opleveren.

De leden van de GroenLinks-PvdA-fractie juichen toe dat Nederland een vooraanstaande positie bekleedt in de *Governmental Advisory Committee* binnen de Internet Corporation for Assigned Names and Numbers (ICANN).
Is de minister bereid om de uitkomsten van de gesprekken die in dit verband worden gevoerd, periodiek aan de Kamer terug te koppelen, mogelijk als paragraaf in de Verzamelbrieven Digitalisering die door de staatssecretaris voor Digitalisering worden opgesteld?

34. Antwoord van het kabinet

De adviezen van de *ICANN Governmental Advisory Committee* (GAC) worden na afloop van de vergaderingen gepubliceerd middels een Communiqué, deze zijn publiek beschikbaar via de website van ICANN[14].

De minister van Economische Zaken is verantwoordelijk voor de inzet in ICANN. Hij zal uw Kamer periodiek informeren over het ICANN-dossier middels de voortgangsbrief over de Strategie Digitale Economie.

Deze leden benadrukken ook dat voor een geloofwaardige positie binnen ICANN het van het grootste belang is om de DNS (Domain Name System)-infrastructuur van Nederland ook in

[14] Zie; Governmental Advisory Committee Official Web Presence; https://gac.icann.org

volledig Nederlands beheer te brengen. Dit geldt al helemaal sinds de AIVD heeft bekendgemaakt dat de voorgenomen (inmiddels beperkte) verhuizing van de DNS-infrastructuur naar een Amerikaanse clouddienst risicovol is (Kamerstuk 26 643, nr. 1272)).

Acht de minister het ook in geopolitieke context van belang dat Nederland laat zien de eigen DNS-infrastructuur te kunnen en willen beheren? Is hij bereid om zich, ook vanuit het geopolitieke belang, constructief in te zetten om de Stichting Internet Domeinregistratie Nederland (SIDN) te helpen in de zoektocht naar een geschikte Nederlandse leverancier, samen met zijn collega's van Binnenlandse Zaken en Economische Zaken conform de unaniem aangenomen motie-Kathmann c.s. (Kamerstuk 26643, nr. 1317)?

35. Antwoord van het kabinet

De minister van BZ staat achter het kabinetsbesluit van 17 januari jl. inzake het .nl domein. In het Kabinetsbesluit van 17 januari jl. inzake de migratie van het domeinregistratiesysteem van het .nl-domein is aangegeven dat SIDN onder strikte voorwaarden de migratie naar de *public cloud* van AWS kan maken voor een beperkt deel van het domeinregistratiesysteem, mits de risico's die door de AIVD in kaart zijn gebracht voor het domeinregistratiesysteem gemitigeerd worden door de maatregelen die door de AIVD zijn voorgesteld. Het kabinet had liever gezien dat SIDN direct gebruik kon maken van een Nederlandse of Europese oplossing zodat de gehele DNS-keten in Nederland kon blijven, maar zo ver bekend is er op dit moment geen geschikte Nederlandse cloudaanbieder.

De ministeries van Economische Zaken en Binnenlandse Zaken en Koninkrijksrelaties zijn bezig om uitvoering te geven aan de aangenomen motie Kathmann, uit het debat 13 maart jl. over overheids-ICT migraties. Hierin is de regering verzocht om in overleg te gaan met SIDN en nationale cloudaanbieders om ook het beperkte deel van de DNS-keten dat naar AWS gaat weer in Nederland te krijgen. Conform het kabinetsbesluit van 17 januari kan SIDN een deel van haar domeinregistratiesysteem naar AWS migreren. Op basis van de aangenomen motie gaan SIDN en de overheid wel verkennen of er een geschikte Nederlandse cloudaanbieder is voor dit deel van het domeinregistratiesysteem om ook het beperkte deel van de DNS-keten dat naar AWS gaat weer in Nederland te krijgen. Voor de zomer wordt uw Kamer geïnformeerd over deze uitkomst.

De leden van de GroenLinks-PvdA-fractie horen graag meer over de dialogen met de Westelijke Balkan, Indo-Pacific en zuidelijk Afrika.

Wat is het doel van de regionale consultaties die de minister benoemt? Hoeveel zijn er reeds uitgevoerd en met welke partijen zijn deze overleggen geweest? Zijn er in dit verband afspraken gemaakt op het gebied van cyberveiligheid, cybercriminaliteit en internet governance?

36. Antwoord van het kabinet

Het ministerie van Buitenlandse Zaken heeft vier regionale cyberdialogen gehouden met de Westelijke Balkan en bereidt regionale dialogen voor met de prioriteitsregio's Zuidelijk Afrika en Zuidoost-Azië. Deelnemers van deze dialogen komen van overheidsorganisaties, denktanks en universiteiten. Het doel van deze regionale consultaties is het vergroten van

het kennisniveau van de deelnemers en het versterken van de (regionale) samenwerking tussen sectoren in de weerbaarheid tegen cyberdreigingen in de brede zin. Daarnaast bieden de dialogen de mogelijkheid om Nederlandse prioriteiten op het gebied van cyberveiligheid onder de aandacht te brengen bij een brede groep landen en hierover in gesprek te gaan.

Tot slot benadrukken de leden van de GroenLinks-PvdA-fractie nogmaals dat Nederland een enorme stempel kan en moet drukken op het digitale wereldtoneel. Het organiseren van de *Global Conference on Cyber Capacity Building* is dan ook bij uitstek een gelegenheid om de Nederlandse expertise waardevol in te zetten.
Kan de minister meer zeggen over de uitkomsten van deze conferentie? Is hij het met deze leden eens dat dergelijke conferenties niet alleen moeten leiden tot discussies, maar ook tot concrete plannen en acties?

37. Antwoord van het kabinet

Tijdens de eerste Global Conference on Cyber Capacity Building in 2023 is de Accra Call aangenomen waarin Nederland samen met de EU en meer dan 50 andere landen en organisaties pleiten voor het incorporeren van cyberweerbaarheid binnen duurzame ontwikkelingsprogramma's. Nederland pleit voor deze aanpak in diverse fora en werkt ook zelf aan het versterken van een geïntegreerde benadering. Zo werkt Nederland via het *Challenge Fund for Youth Employment* aan het opleiden van jongeren in cyber security in de focusregio's en draagt daarmee bij aan zowel onderwijs als veiligheid. Tijdens de aankomende conferentie in mei 2025 zal het ministerie van Buitenlandse Zaken een sessie organiseren over het belang van het investeren in cyberveiligheid in digitale klimaatoplossingen.

De leden van de GroenLinks-PvdA-fractie danken alle betrokken ambtenaren hartelijk voor de beantwoording.

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben kennisgenomen van de brief over de voortgang van de Internationale Cyberstrategie en hebben daarover enkele vragen en opmerkingen.

Deze leden zien de toenemende dreiging van offensieve cyberactiviteiten door de veranderende geopolitieke realiteit. Vooral China en Rusland zijn er in toenemende mate op uit om ons te destabiliseren.

Deze leden vragen het kabinet in hoeverre de toenemende cyberdreiging vanuit Chinese en Russische cyberoperaties komt of dat het om een bredere trend gaat.

38. Antwoord van het kabinet

China en Rusland hebben een hoog soortelijk gewicht in de toenemende cyberdreiging, maar zijn niet de enige actoren. Ook andere landen, zoals Iran en Noord-Korea, investeren in hun offensieve cyberprogramma's. Uit de jaarverslagen van AIVD en MIVD blijkt dat het aantal landen dat grotere cybercapaciteiten ontwikkelt, toeneemt. Steeds meer landen

die voorheen nog geen offensieve cyberprogramma's hadden, investeren nu ook in zulke programma's. Daarvoor krijgen zij hulp van bondgenoten of ze kopen geavanceerde commerciële offensieve cybercapaciteiten in, zoals bijvoorbeeld spyware. Ook is een toename waarneembaar in de activiteiten van niet-statelijke actoren zoals cybercriminelen.

Van alle cyberdreigingen heeft digitale sabotage potentieel de grootste impact op Nederland, omdat dit kan leiden tot verstoringen van militaire operaties, economische schade en maatschappelijke ontwrichting. In de laatste jaren zagen de AIVD en MIVD verschillende buitenlandse cyberoperaties, waaronder van Rusland en China, die gericht waren op Europese en NAVO-doelen, vaak met als doel uiteindelijk vitale infrastructuur te kunnen saboteren in tijden van conflict.

De leden van de VVD-fractie vragen het kabinet wat de knelpunten zijn voor het verder verbeteren van de Nederlandse en Europese digitale slagkracht. Deze leden lezen dat Nederland het initiatief neemt binnen de EU om met gezamenlijke maatregelen tegen cyberdreigingen te komen. Welke extra voorstellen gaat het kabinet doen om onze weerbaarheid te verhogen? Ook vragen deze leden hoe het kabinet binnen de EU inzet op innovatie voor cyber en cybersecurity.

39. Antwoord van het kabinet

Het kabinet zet zich er via de verschillende Europese gremia actief voor in de digitale weerbaarheid in de EU te vergroten. Zo is Nederland aangesloten bij het *European Cyber Crisis Liaison Officers Network* (CyCLONe) en het *Computer Security Incident Response* (CSIRT) netwerk, waarbinnen lidstaten zich voorbereiden op grootschalige cybercrises en -incidenten. Ook verwelkomt het kabinet het initiatief van de Europese Commissie om de Blueprint inzake Grootschalige Cyber Incidenten te herzien; het BNC-fiche van dit voorstel is 4 april jl. met uw Kamer gedeeld.[15]

In lijn met de NLCS en de NIS2-richtlijn (Cyberbeveiligingswet) fungeert het NCSC sinds 17 oktober 2024 als Single Point of Contact (SPOC), wat betekent dat het NCSC voor Nederland het internationale aanspreekpunt is op het gebied van cybersecurity. Het NCSC werkt in verschillende nationale en internationale samenwerkingsverbanden, zowel publiek als privaat, intensief samen met diverse organisaties aan het verhogen van de digitale weerbaarheid.

Daarnaast zal de digitale weerbaarheid in de gehele EU sterk toenemen met onder meer de aanstaande implementatie van de NIS2-richtlijn in de Cyberbeveiligingswet (Cbw) en de uitvoering van de *Cyber Resilience Act* (CRA). Daarnaast is het voor het kabinet van belang dat de complexiteit en overlap binnen het Europese cybersecuritylandschap wordt verminderd. Het kabinet zet zich daarom in Europees verband actief in om samenhang en harmonisatie ten aanzien van cybersecurity wet- en regelgeving te vergroten.

Tot slot pleit het kabinet binnen de EU actief voor het versterken van de samenwerking op cybersecurity-innovatie. Daarbij hoort het hanteren van *cybersecurity-by-design* als leidend principe in de Europese industrie, het vergroten van de samenwerking tussen overheden,

[15] Kamerstuk 22112, nr. 4018 | Overheid.nl > Officiële bekendmakingen

bedrijven, investeerders, overheden en kennisinstellingen, en het versterken van het Europees kenniscentrum voor cyberbeveiliging (ECCC) en het netwerk van nationale coördinatiecentra (NCC's). Het NCC-NL verbindt de Nederlandse cybersecuritygemeenschap aan Europese partijen voor gezamenlijke inschrijving op EU-subsidietrajecten. In algemene zin pleit het kabinet voor een Europese technologiestrategie, zodat gerichter wordt geïnvesteerd in sleuteltechnologieën zoals cybersecurity, onder meer via de D9+ coalitie. Tijdens de top die het kabinet afgelopen maart organiseerde hebben de verantwoordelijke ministers zich gezamenlijk uitgesproken voor het verbinden van ecosystemen voor digitale innovatie, en het mobiliseren van meer privaat kapitaal voor het versterken van het Europese digitaal concurrentievermogen.

Parallel aan het versterken van de weerbaarheid ziet het kabinet ook graag dat de EU meer werk maakt van het ontmoedigen van kwaadwillende actoren d.m.v. diplomatieke inzet. Zie voor een verdere toelichting op deze inzet ook het antwoord op vraag 1.

De leden van de VVD-fractie vinden recente grote cyberaanvallen op universiteiten zorgelijk. Deze leden vragen wat er nodig is om Nederlandse universiteiten beter te beschermen tegen cyberaanvallen.

40. Antwoord van het kabinet

De hogescholen en universiteiten zetten via bestuurlijke afspraken met OCW in op het verhogen van de cyberweerbaarheid. Zij nemen concrete maatregelen om de cyberweerbaarheid te versterken en hebben hierop in de afgelopen jaren grote stappen gezet, zowel op instellingsniveau als met de sector als geheel. De minister heeft uw Kamer recentelijk geïnformeerd over de stand van zaken ten aanzien van de aanpak ter versterking van de cyberweerbaarheid in het vervolgonderwijs en over zijn besluit om de hogescholen en universiteiten aan te wijzen als essentiële of belangrijke entiteit bedoeld in de Cyberbeveiligingswet en de instellingen daarmee onder de reikwijdte van de aanstaande wet te brengen. Dit besluit wordt op dit moment verder uitgewerkt met alle betrokken partijen. De minister van OCW zal uw Kamer later dit jaar informeren over deze nadere uitwerking.

Er zijn ook steeds vaker cyberaanvallen waardoor wereldwijd bedrijven stilvallen. Deze leden vragen het kabinet hoe zij de risico's op cyberaanvallen met wereldwijde gevolgen wil verkleinen. De leden van de VVD-fractie zijn met name bezorgd over cyberveiligheid in kritieke sectoren.

Hoe zet het kabinet zich ervoor in om onze kritieke sectoren weerbaar te maken tegen cyberaanvallen?

41. Antwoord van het kabinet

Op dit moment werkt het kabinet aan de implementatie van de NIS2-richtlijn in de Cyberbeveiligingswet en de daarop te baseren nadere wetgeving. Deze wetgeving draagt bij aan een hoger niveau van cybersecurity in de verschillende in de NIS2-richtlijn genoemde kritieke sectoren. Zo worden organisaties, die krachtens de Cyberbeveiligingswet als essentiële of belangrijke entiteit worden aangemerkt, verplicht om passende en evenredige

maatregelen te nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. Daarnaast zijn deze organisaties bij significante incidenten meldplichtig en hebben zij recht op bijstand van het NCSC.

De leden van de VVD-fractie zijn positief dat sancties opgelegd worden aan Russische cybercriminelen die diensten leveren voor de Russische inlichtingendiensten.

Deze leden vragen het kabinet of het sanctioneren van cybercriminelen ook toepasbaar is op andere landen met een offensief cyberprogramma tegen Nederland, zoals op China. Wat zijn hierbij de overwegingen?

42. Antwoord van het kabinet

Het Europese cybersanctieregime is landenonafhankelijk en gericht op personen en entiteiten. Sinds de oprichting van het regime in 2019 zijn er individuen en bedrijven gesanctioneerd uit verschillende landen, waaronder ook uit China en Noord-Korea. Sinds 2020 zijn er sancties aangenomen tegen in totaal 14 personen en 4 entiteiten. In 2024 zijn op Nederlandse voordracht sancties aangenomen tegen een aantal vooraanstaande Russische cybercriminelen. Het kabinet is er voorstander van ook te kijken naar de mogelijkheid van sanctionering van cybercriminelen uit andere landen. Voorwaarde is dat de activiteiten van die criminelen een ontwrichtend effect hebben binnen de EU. Voor het aannemen van sancties in EU-verband is instemming van alle lidstaten vereist en het verkrijgen van die instemming is geregeld een uitdaging.

De leden van de VVD-fractie lezen dat Nederland financiering heeft verstrekt aan Oekraïne voor toegang tot het internet via Starlink-satellieten.

Deze leden vragen hoe het kabinet kijkt naar Elon Musk's dreigement om Oekraïne toegang te ontzeggen tot Starlink. Ondersteunt het kabinet Oekraïne op het moment om te komen tot alternatieven, indien Starlink zou wegvallen? Waar zou het concreet om gaan?

43. Antwoord van het kabinet

Het kabinet ondersteunt Oekraïne momenteel in het vinden van verschillende alternatieven. Ook worden met Nederlandse financiering via de NAVO *Oneweb* terminals aangeschaft en draagt Nederland via het NAVO *Ukraine Comprehensive Assistance Package* (UCAP) bij aan de aanschaf van alternatieve satellietsystemen. Met bijdrage aan dit NAVO UCAP project wordt het bestaande netwerk uitgebreid met additionele terminals en de daarvoor noodzakelijke *airtime*, reserveonderdelen, ondersteuning en trainingen.

Deze alternatieven kunnen helpen om de continuïteit van vitale communicatie-infrastructuur voor Oekraïne te waarborgen, vooral in het licht van de huidige geopolitieke situatie en de afhankelijkheid van satellietverbindingen.

De leden van de VVD-fractie lezen dat het kabinet buiten de EU en NAVO samenwerking met partnerlanden wil uitbreiden om landen met een offensief cyberprogramma beter tegen te gaan. Hiervoor zijn cyberconsultaties uitgevoerd met verschillende landen.

Deze leden vragen of er concrete suggesties uit deze consultaties naar voren zijn gekomen om bestaand beleid aan te scherpen. Hoe wil het kabinet de samenwerking met die landen verder vormgeven?

44. Antwoord van het kabinet

Het kabinet is in dialoog met invloedrijke landen buiten de EU en NAVO zoals Japan en Zuid-Korea om de samenwerking op het tegengaan van digitale dreigingen te intensiveren. Tegelijkertijd wordt operationele samenwerking tussen bijvoorbeeld politiediensten, krijgsmachten en nationale cybersecuritycentra aangehaald. Om kwaadwillend statelijk cybergedag tegen te gaan, is het van belang dat zoveel mogelijk landen zich uitspreken tegen andere landen die handelen in strijd met het VN normatief kader voor statelijk gedrag in het cyberdomein. Dat kan bijvoorbeeld via publieke verklaringen of technische rapporten gericht op mitigatie van cyberdreigingen.

Deze leden vragen ook in hoeverre er ingezet wordt op het tegengaan van offensieve cyberprogramma's bij de diensten. Is deze inzet voldoende?

45. Antwoord van het kabinet

Het kabinet zet in op zowel internationale samenwerking als de inzet van de AIVD en MIVD. De diensten doen inlichtingenonderzoeken naar offensieve cyberoperaties die gericht zijn tegen Nederlandse en bondgenootschappelijke belangen. De informatie over intenties en capaciteiten van malicieuze actoren helpt het kabinet om de kosten voor aanvallers te verhogen, samen met bondgenoten.

Hoewel de diensten digitale aanvallen niet altijd kunnen voorkomen of onderkennen, worden cyberdreigingen zoals de recente Chinese *Salt Typhoon*-aanvallen nauwgezet gevolgd en gerapporteerd.

De inzet van de diensten wordt versterkt door de Tijdelijke wet cyberoperaties (2024), die hun bevoegdheden sneller en effectiever maakt. Deze wet bevat bindend toezicht door de CTIVD, die operaties kan stopzetten en gegevens kan laten vernietigen.

De leden van de VVD-fractie benadrukken dat vrijheid en veiligheid op het internet centraal staan. Zij zijn bezorgd over de wens van een aantal landen om een coördinerende rol van onder andere de VN en de Internationale Telecommunicatie Unie (ITU) te hebben op het internet. Het is goed dat Nederland zich hiertegen keert.
Deze leden vragen hoe het kabinet zich blijvend gaat verzetten om geen tractie te geven aan dergelijke ideeën. Hoe benadrukt het kabinet internationaal de noodzaak van een vrij multistakeholder model?

46. Antwoord van het kabinet

Nederland benadrukt richting deze landen dat het centraliseren van *internet governance* bij de ITU geen oplossing is voor deze zorgen, maar juist de stabiliteit en politieke neutraliteit van het mondiale internet in gevaar brengt. Onder leiding van Nederland heeft de ITU afgelopen jaar tijdens de *World Telecommunication Standardization Assembly* (WTSA) in

Delhi een tweetal resoluties aangenomen die de rol van *multistakeholder* organisaties in het beheer van de publieke kern van het internet bevestigen.

Tijdens het voorzitterschap van de *Freedom Online Coalition (*FOC) in 2024 heeft Nederland erop ingezet om hiervoor zoveel mogelijk internationale steun te verkrijgen, met als resultaat onder meer een naar tevredenheid stemmend Global Digital Compact[16] dat in september 2024 op VN-niveau met consensus is aangenomen.

Ook in 2025 zet Nederland in op versterkte coördinatie met gelijkgezinde landen binnen de FOC en anderszins richting de herziening van de *World Summit on the Information Society* (WSIS+20 review). Tijdens deze WSIS+20 review worden o.a. de bestaande VN-afspraken over *internet governance* heronderhandeld, hetgeen grote impact kan hebben op de toekomst van het *multistakeholder* model. Daarnaast is de Nederlandse overheid en een grote Nederlandse *multistakeholder*-delegatie al jaren actief betrokken bij het *Internet Governance Forum* waar belanghebbenden van over de hele wereld bijeenkomen om vraagstukken rond het beheer van het internet op gelijke voet met elkaar te bespreken. Middels het ministerie van Economische Zaken ondersteunt Nederland dit Forum ook financieel.

De leden van de VVD-fractie zien statelijke desinformatie als een dreiging voor onze open en democratische samenleving. Desinformatiecampagnes van andere staten met als doel om de Nederlandse samenleving te beïnvloeden, moeten gestopt worden.
Daarom vragen deze leden hoe het kabinet zich binnen Nederland en de EU inzet om statelijke desinformatie tegen te gaan. In hoeverre kan zij statelijke desinformatie goed tegengaan met het huidige instrumentarium?

47. Antwoord van het kabinet

Nederland zet zich in de EU actief in voor een sterke aanpak van statelijke desinformatie. In 2023 is in de EU de implementatie van de *Foreign Information Manipulation and Interference* (FIMI) *Toolbox* afgerond. Hiermee kan op systematische wijze worden gereageerd op FIMI-dreigingen en incidenten, waaronder statelijke desinformatie. Daarnaast is Nederland lid van het *EU Rapid Alert System* (RAS) voor informatie-uitwisseling over en signalering van statelijke desinformatie. Nederland maakt actief gebruik van deze instrumenten om gezamenlijk op te treden tegen statelijke desinformatie. Binnen Nederland wordt gewerkt aan een aantal parallelle werksporen voor een geïntegreerde aanpak van statelijke desinformatie. Uw Kamer is hierover geïnformeerd in de Rijksbrede strategie voor effectieve aanpak van desinformatie en de daaropvolgende Voortgangsbrief.[17]

[16] VN Pact for the Future en Global Digital Compact
[17] Zie: *Rijksbrede strategie effectieve aanpak van desinformatie, TK 2022–2023, 30 821, nr. 173* en *Voortgangsbrief Rijksbrede strategie voor de effectieve aanpak van desinformatie en aankondiging nieuwe acties, TK 2023–2024, 30 821, nr. 230*

Vragen en opmerkingen van de leden van de NSC-fractie

De leden van de NSC-fractie hebben met interesse kennisgenomen van de stukken bijgaand dit schriftelijk overleg. Deze leden hebben op basis hiervan nog enkele vragen.

Het lid Omtzigt heeft op 5 maart jl. een motie op stuk nummer 21 501-20, nr. 2198, ingediend. Deze motie riep het kabinet ertoe op om een solide basis te scheppen voor de privaat-publieke samenwerking op cyberterrein, het Defensie Cyber Commando (DCC) een adequaat mandaat te geven en het te versterken.

De gleden van de NSC-fractie vragen hoe het met de uitvoering van deze motie staat, gezien de actuele dreiging vanuit Rusland.

48. Antwoord van het kabinet

Het kabinet erkent het belang van de AIVD en MIVD in het vergaren van inlichtingen over cyberdreigingen. Deze inlichtingen helpen bij het vormgeven van het cybersecuritybeleid en het nemen van maatregelen tegen aanvallers, al dan niet met bondgenoten. Hoewel niet alle incidenten kunnen worden voorkomen, zoals recente voorbeelden in de VS rondom Chinese hackersgroep *Salt Typhoon* aantonen, rapporteren de diensten jaarlijks over hun bevindingen.

Een eenduidig kader voor publiek-private samenwerking door de diensten op cyberterrein wordt expliciet meegenomen in de herziening van de Wiv. De huidige wet biedt wel een basis, maar duidelijke kaders ontbreken. Het kabinet streeft naar een wettelijk kader dat geen apart beleid meer nodig maakt.

De Defensienota's 2022 en 2024 voorzien in de groei van de operationele cybercapaciteit van het Defensie Cybercommando (DCC). De personeelsstrategie beoogt het reservistenbestand snel uit te breiden. Daarnaast wordt met de aankomende Defensie Cyberstrategie een proactieve aanpak tegen statelijke cybercampagnes nagestreefd. In de strategie worden ook de inzet van de krijgsmacht (i.c. het DCC) naast contra-inlichtingenactiviteiten van de MIVD genoemd. Het DCC heeft geen zelfstandige bevoegdheden. De regering besluit tot inzet van het DCC en eventuele bevoegdheden zijn afhankelijk van de grondslag voor de inzet.

De leden van de NSC-fractie vragen in samenhang hiermee in hoeverre er al afspraken gemaakt zijn met het Nederlandse bedrijfsleven om in geval van cyberaanvallen bij te springen. Deze leden hebben in de brief van de minister gelezen dat de Tijdelijke Wet Cyberoperaties nog niet volledig wordt toegepast, omdat de CTIVD in verband met huisvesting en daaruit volgend capaciteitsgebrek slechts beperkt toezicht kan houden. Deze leden vragen op welke termijn de minister verwacht dat dit probleem wordt opgelost.

49. Antwoord van het kabinet

Hiervoor verwijs ik u naar antwoord op vraag 8.
De AIVD en MIVD werken samen met het Nederlandse bedrijfsleven op cybergebied. Deze samenwerking omvat een wederzijdse uitwisseling van technische gegevens, zoals

kenmerken van infrastructuur en malware gebruikt bij cyberaanvallen. Bedrijven fungeren als informant, terwijl de diensten gegevens verstrekken om de digitale weerbaarheid van Nederland en zijn bondgenoten te versterken.

De leden van de NSC-fractie hebben er ook kennis van genomen dat het kabinet in de komende tijd de samenwerking met belangrijke partnerlanden op het gebied van cyber wil intensiveren. Een van de betreffende landen is de VS.

Deze leden vragen in hoeverre de actuele ontwikkelingen rond de Trump-administratie hiervoor in de toekomst een obstakel zouden kunnen vormen.

50. Antwoord van het kabinet
Hiervoor verwijs ik u naar het antwoord op vraag 1.

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben kennisgenomen van de voortgang van de internationale cyberstrategie en de ontwikkelingen op het gebied van hybride dreigingen en geopolitieke verschuivingen. Zij hebben hierover enkele vragen en opmerkingen.

Deze leden constateren dat de geopolitieke dynamiek snel verandert, onder andere door de toegenomen hybride dreigingen vanuit Rusland en de inmenging van grote technologiebedrijven in Westerse democratieën.

Deze leden vragen de minister of de huidige cyberstrategie nog actueel is en of er, gezien de veranderende wereldorde, een herziening nodig is.

51. Antwoord van het kabinet
Hiervoor verwijs ik u naar het antwoord op vraag 1.

Zij vragen de minister of de recente ontwikkelingen rondom platform X en de invloed van Elon Musk worden meegenomen in de strategische afwegingen van het kabinet en op welke manier dit leidt tot wijzigingen of aanscherpingen in de internationale cyberstrategie.

52. Antwoord van het kabinet
Zoals ook verwoord in het antwoord op vraag 1, neemt het kabinet alle relevante actuele geopolitieke ontwikkelingen mee in de uitvoering van de internationale cyberstrategie. Hier vallen ontwikkelingen op het gebied van online platforms en uitlatingen van eigenaren van die platforms ook onder. Op dit moment geven deze ontwikkelingen geen aanleiding om de cyberstrategie aan te passen.

In het verlengde daarvan vragen deze leden of de bezuinigingen op cybersecurity binnen de begroting van Buitenlandse Zaken heroverwogen zouden moeten worden, gezien het toenemende belang van digitale veiligheid.

53. Antwoord van het kabinet

De bezuinigingen op het ministerie van Buitenlandse Zaken hebben een zekere weerslag op de uitvoering van de internationale cyberstrategie. De taakstelling beperkt de beschikbare middelen voor programma's ter versterking van de cyberweerbaarheid in opkomende landen.

Hierdoor is het essentieel om scherpe keuzes te maken, middelen strategisch in te zetten en de samenwerking te intensiveren tussen ministeries onderling en met partners in binnen- en buitenland. Zo trekt het ministerie van Buitenlandse Zaken nauw op met het RVO, het NCSC en NCC-NL om aan te sluiten bij EU-initiatieven zoals de *Global Gateway*-strategie, om zo met beperkte middelen toch een bijdrage te leveren aan de cybercapaciteitsopbouw in prioriteitsregio's.

Daarnaast vragen deze leden of de Nederlandse inlichtingendiensten onder de huidige Amerikaanse regering nog voldoende in staat zijn om effectief samen te werken met hun Amerikaanse partners. Zij vragen of de interoperabiliteit en informatie-uitwisseling door de politieke dynamiek in de Verenigde Staten wordt belemmerd en welke stappen het kabinet onderneemt om deze samenwerking aan te passen.

54. Antwoord van het kabinet

De toenemende geopolitieke spanningen en onzekerheden benadrukken het belang van de inlichtingendiensten. Internationale samenwerking, inclusief met de VS, is cruciaal voor de nationale en internationale veiligheid. De AIVD en MIVD werken regelmatig met internationale partners en wegen alle relevante omstandigheden mee bij hun werk. Het kabinet kan echter geen details vrijgeven over specifieke inlichtingenposities of gegevensuitwisseling.

De leden van de D66-fractie constateren dat er grote behoefte bestaat aan goed opgeleid IT-talent om Nederland te wapenen tegen cyberdreigingen.

Kan het kabinet aangeven of zij zeker weet dat de aangekondigde bezuinigingen op hoger onderwijs en wetenschap niet ten koste gaan van deze opleidingen ten behoeve van nationale veiligheid? Kan zij voorts aangeven in hoeverre IT-gerelateerde opleidingen op hogescholen en universiteiten zullen krimpen door de voorgenomen beperking op Engelstalige bacheloropleidingen?

55. Antwoord van het kabinet

Het kabinet heeft besloten te bezuinigen op het hoger onderwijs en de wetenschap om investeringen in andere maatschappelijke doelen mogelijk te maken, zoals defensie, veiligheid en bestaanszekerheid. Het kabinet acht de bezuinigingen uitvoerbaar en realistisch. Universiteiten en hogescholen hebben bestedingsvrijheid en beslissen dan ook zelf hoe zij de bezuinigingen vormgeven binnen hun instelling. Dit hangt samen met de (wettelijke) autonomie die zij hebben over hun eigen onderwijs en onderzoek, zij bepalen welk onderwijs ze aanbieden. Het kabinet kan dus geen garanties geven dat een bepaalde opleiding(sector) niet wordt geraakt door de bezuinigingen. Het kabinet verwacht wel van

onderwijsinstellingen dat zij in gezamenlijkheid besluiten over het opleidingsaanbod nemen en maatschappelijke belangen daarin meewegen.

In het wetsvoorstel Wet internationalisering in balans (WIB) wordt de toets anderstalig onderwijs voorgesteld. Opleidingen kunnen toestemming voor anderstalig onderwijs krijgen van de minister van OCW voor opleidingen die doelmatig anderstalig zijn. De WIB kent daarvoor vier doelmatigheidscriteria: regionale omstandigheden, de arbeidsmarkt, internationale uniciteit en internationale positionering van de opleiding of een traject binnen een opleiding. De minister van OCW wordt bij zijn beoordeling geadviseerd door de Commissie doelmatigheid hoger onderwijs. IT-gerelateerde opleidingen op hogescholen en universiteiten dienen in hun aanvraag te motiveren dat zij aan één van die criteria voldoen.

Het is overigens evident dat de techniek een van de grote tekortsectoren in de arbeidsmarkt is. Desondanks kan het kabinet op dit moment niet vooruitlopen op de resultaten van deze toets voor individuele opleidingen. Hierop vooruitlopen zou een vorm van schaduwtoetsing opleveren. De minister van OCW gaat graag met uw Kamer in debat over de precieze invulling van deze criteria bij de parlementaire behandeling van het wetsvoorstel.

De leden van de D66-fractie maken zich verder zorgen over de gevolgen van de aangekondigde bezuinigingen op het postennet voor het tegengaan van desinformatie en het bevorderen van cyberveiligheid in het mondiale Zuiden.

Zij vragen de minister hoe deze bezuinigingen zich verhouden tot de groeiende invloed van China en Rusland in onder andere Afrika en Zuid-Amerika. Hoe verklaart het kabinet de behoefte van China, India en Rusland om hun postennetwerken uit te breiden, waar Nederland die juist laat krimpen, zo vragen deze leden.

56. Antwoord van het kabinet

De taakstelling op onze ambassades, consulaten en permanente vertegenwoordigingen in het buitenland is onderdeel van het regeerprogramma. Dit leidt ook tot een verminderde bezetting van het diplomatieke netwerk. Momenteel wordt bezien hoe deze bezuiniging ingevuld kan worden. Daarbij wordt ook meegenomen hoe het postennet optimaal en blijvend kan worden ingezet voor het behartigen van Nederlandse belangen in een veranderend geopolitiek landschap.

Voorts vragen zij in hoeverre de diplomatieke vertegenwoordigingen nog voldoende worden uitgerust om anti-Westerse desinformatiecampagnes in deze regio's tegen te gaan.

57. Antwoord van het kabinet

Nederland blijft zich inzetten voor het tegengaan van desinformatie, onder meer via ondersteuning van onafhankelijke journalistiek in de Sahel en West-Afrika. Ook steunt Nederland de EU inzet op dit vlak, waaronder het monitoren van het informatiedomein in Sub-Sahara Afrika en het bevorderen van positieve beeldvorming over de EU.

Voor het tegengaan van anti-Westerse desinformatiecampagnes in het mondiale zuiden worden relevante counternarratieven op verschillende manieren uitgedragen, zoals via externe kanalen van ambassades en diplomatieke en informele kanalen.
Het ministerie van Buitenlandse Zaken onderzoekt momenteel hoe met de beschikbare middelen de inzet van de posten om desinformatie tegen te gaan strategischer gecoördineerd kan worden. Hierbij wordt ook gekeken naar het inzetten van middelen zoals het bezoekersprogramma en publieksdiplomatie (KPF non-ODA).

Wat betreft de EU-samenwerking vragen de aan het woord zijnde leden hoe de minister zich inzet om de samenwerking op het gebied van cyberdreigingen binnen de Europese Unie te verbeteren.

58. Antwoord van het kabinet
Hiervoor verwijs ik u graag naar het antwoord op vraag 39.

Zij vragen de minister welke obstakels er zijn bij de informatie-uitwisseling tussen EU-lidstaten en welke concrete stappen worden gezet om deze barrières weg te nemen.

59. Antwoord van het kabinet
Met de inwerkingtreding van NIS2-richtlijn én de nationale wetgeving ter implementatie daarvan wordt bevorderd dat informatie over dreigingen en incidenten kan worden uitgewisseld tussen organisaties in EU-lidstaten. Uiteraard zijn deze organisaties verplicht om in het kader van verstrekking van informatie wettelijke kaders zoals de AVG in acht te nemen.

De leden van de D66-fractie lezen dat de minister schrijft: “Tot slot heeft het kabinet Oekraïne bijgestaan zich beter te wapenen tegen de Russische cyberdreiging; zo financierde Nederland cyberveiligheidsproducten en toegang tot het internet via Starlink-satellieten.” Deze leden zijn uiteraard groot voorstander van elke vorm van steun aan de Oekraïners, die ook strijden voor onze veiligheid, maar zijn wel bezorgd over de afhankelijkheid van Starlink in het licht van de onberekenbare Amerikaanse regering. Hoewel de VS stelt niet voornemens te zijn Oekraïne af te sluiten van Starlink, hebben de recente ontwikkelingen rondom wapenleveranties en het delen van inlichtingen laten zien dat er niet onvoorwaardelijk op de Amerikanen kan worden gerekend. Welke alternatieven voor Starlink bestaan er, als de Oekraïense toegang hiertoe wel wordt beperkt, zo vragen de leden van de D66-fractie. Hoe beschouwt het kabinet in dit licht de capaciteiten van Eutelsat? Voorts vragen zij of het kabinet bereid is te investeren in Europese alternatieven en hoe Nederland hieraan kan bijdragen.

60. Antwoord van het kabinet
Hiervoor verwijs ik u ook naar het antwoord op vraag 18 en 43.

De Europese Commissie beschouwt alle mogelijkheden om Oekraïne te ondersteunen, ook op het gebied van satellietcommunicatiesystemen (SATCOM). Om strategische afhankelijkheden op de korte termijn te beperken, zet de Europese Commissie in op de verbreding naar commerciële SATCOM aanbieders op de Europese markt. Deze diensten

kunnen dan ook aan Oekraïne beschikbaar gesteld worden. Eutelsat Oneweb is een relatief eenvoudig te gebruiken commerciële *Low Earth Orbit* constellatie net als Starlink. Dit systeem en het Delta-systeem hebben in principe soortgelijke functionaliteiten en mogelijkheden. Daarnaast werkt de Europese Commissie op de langere termijn (vanaf 2030) onder het Europees Ruimtevaartprogramma aan het ontwikkelen van autonome satellietcommunicatie voor overheidsinstellingen. Deze capaciteiten zouden eveneens voor militair gebruik bestemd zijn. Nederland onderschrijft het belang van de diversificatie van deze markt. Dit wordt gewaarborgd door diensten te spreiden en Europese ontwikkelingen op dit vlak te stimuleren.

Tot slot vragen deze leden naar de inzet van Nederland bij de oprichting van een VN-mechanisme voor de implementatie van een normatief kader voor verantwoordelijk statelijk gedrag in het cyberdomein. Zij vragen de minister wat de verwachting van het kabinet is over de onderhandelingen die in de zomer van 2025 zullen plaatsvinden. Welke prioriteiten stelt Nederland in deze onderhandelingen en hoe worden die afgestemd met Europese partners, zo vragen zij.

61. Antwoord van het kabinet

Het mandaat van het huidige VN-mechanisme om te komen tot een permanent VN-mechanisme op *cyber* in het veiligheidsdomein loopt af in de zomer van 2025. In het krachtenveld van deze onderhandelingen staan de onderhandelingsposities van democratische en autocratische landen tegenover elkaar. De EU zet zich met steun van het kabinet, en samen met andere gelijkgezinde landen, in voor een actiegericht vervolgprogramma (*Programme of Action)*. Dit initiatief richt zich op de uitvoering en naleving van afspraken over verantwoordelijk statelijk gedrag in het cyberdomein. Daarnaast maakt het kabinet zich er hard voor dat in de VN-discussies niet alleen de stemmen van staten maar ook die van maatschappelijke organisaties, academici en de private sector gehoord worden.

Vragen en opmerkingen van de leden van de BBB-fractie

De leden van BBB-fractie hebben kennisgenomen van de brief over de voortgang van de Internationale Cyberstrategie. Zij zien met zorg een paar ontwikkelingen met betrekking tot het internationale cyberbeleid en zijn daarom ook tevreden dat hier vanuit het kabinet aandacht voor is.

Deze leden vinden het bedreigend dat Russische en Chinese hackers, maar ook andere statelijke en niet-statelijke actoren ons treffen. Ook op dit vlak moet Nederland zich weerbaarder kunnen opstellen en in Europees verband onderzoeken of wij ook minder afhankelijk kunnen zijn van datacenters, iclouds en andere systemen van derde landen. Op dit vlak moeten Nederland en Europa ook onafhankelijker kunnen opereren, net als dat met defensie op dit moment opgepakt wordt.

De leden van de BBB-fractie vinden het goed dat Nederland Oekraïne heeft bijgestaan zich beter te weren tegen Russische cyberdreiging. Dit gebeurde onder meer door het toegang verlenen tot het internet via Starlink-satellieten. Deze leden vinden het echter verstandig om ook voorbereid

te zijn op een samenleving waarin wij niet meer van Starlink of andere buitenlandse satelliet- en ruimtevaartprogramma's afhankelijk zijn, maar ook meer op eigen benen kunnen staan. Daarom dienden de leden van de BBB-fractie hierover vorige week een motie in.

De leden van de BBB-fractie maken zich zorgen over het feit dat Nederland en de EU achterlopen op het vlak van AI. Het is dan ook goed dat Nederland internationaal wordt erkend als belangrijke speler op het gebied van verantwoorde inzet van AI. Het is dan eigenlijk nog sterker om flink in te zetten op een eigen ontwikkeling van AI, dan op het inperken van de mogelijkheden die dit biedt, want dat werkt averechts. Ook Nederlandse bedrijven zouden op dit vlak een voortrekkersrol moeten kunnen vervullen. De leden van de BBB-fractie zijn voor het tegengaan van statelijke desinformatie en voor het behoud van een open, vrij en veilig internet. Censuur moet worden voorkomen, waarbij er een spanningsveld bestaat tussen censuur en hoe om te gaan met desinformatie. Een gedigitaliseerde samenleving kent volgens deze leden veel voordelen, maar deze moet ook beschermd worden tegen cyberkwetsbaarheden, zonder daarbij in beperkingen en censuur te vervallen. Dat is een lastig krachtenspel.

Met zorg lazen deze leden het artikel 'Nederland is een paradijs voor cybercriminelen' in het Parool van 20 maart jl., waarin de keerzijde wordt genoemd van het grote aantal datacenters in Nederland. De leden van de BBB-fractie vragen of dit ook haar uitstraling heeft op de cyberveiligheid van statelijke en niet-statelijke actoren en hun infiltratie in Nederland.

62. Antwoord van het kabinet

Nederland heeft een sterke digitale infrastructuur en er staan veel datacenters op ons grondgebied. De zorgen omtrent datacenters en het faciliteren van criminaliteit worden door het kabinet onderkend. De minister van JenV heeft de Kamer toegezegd om in het voorjaar 2025 te komen met een verkenning naar mogelijke oplossingen rondom de problematiek van zgn. '*bullitproof hosting'* en '*bad hosting'*. Een van de onderdelen van deze verkenning is dat er gekeken wordt naar hoe een 'ken je klant-principe' wettelijk verankerd zou kunnen worden, zodat een beter zicht op de keten van klanten mogelijk is. Dit 'ken je klant-principe' helpt tegen het schadelijke gebruik van de Nederlandse netwerken, statelijk of crimineel. Kwaadwillenden blijven immers het liefst zo anoniem mogelijk. Door implementatie van een dergelijke maatregel kunnen ook de buitenlandse hosting *resellers*, die een groot deel van de schade faciliteren, worden geweerd bij Nederlandse bedrijven zoals datacentra (colocatie) en hosting providers.
Cybercriminelen kunnen een server in een bepaald land gebruiken als tussenstation voor internationale cyberaanvallen. In de regel heeft een datacentrum geen zicht op de inhoud van een server. Hosting providers hebben dat wel, met de kanttekening dat het zicht deels afhankelijk is van het type dienst of server. Het NCSC kan *Notice and Take Down* (NTD) verzoeken doen aan hosting partijen om een domein of systeem dat wordt gebruikt door kwaadwillenden uit te schakelen. Een hostingpartij kan dit verzoek weigeren (*bulletproof hosting*). Het NCSC kan een beheerder of *Internet Service Provider* (ISP) dus wel informeren, maar niet verplichten.

Vragen en opmerkingen van de leden van de SGP-fractie

De leden van de SGP-fractie hebben de stukken over de voortgang van de Internationale Cyberstrategie (ICS) ontvangen, danken het kabinet voor het toezenden daarvan en hebben nog enige vragen en opmerkingen.

Kan het kabinet schetsen hoe zij de cyberafschrikking ziet? Waar is meer accent op komen te liggen, zo vragen de leden van de SGP-fractie.

63. Antwoord van het kabinet

Afschrikking in het cyberdomein is een onderdeel van het cyberbeleid dat gericht is op het ontmoedigen en het verhogen van de kosten van cyberaanvallen. Afschrikking is op zich onvoldoende om de cyberdreiging te mitigeren. De dreiging van statelijke cyberaanvallen op vitale processen is aanhoudend en omvangrijk en vraagt om brede inzet van instrumenten. Het is van groot belang om weerbaarheid hiertegen te versterken en te pogen kwaadwillende actoren af te schrikken en te ontmoedigen. Daarvoor is een geïntegreerde inzet van inlichtingen, verstoringsoperaties, militaire instrumenten en diplomatieke middelen nodig. Een deel van de activiteiten onder deze noemers zijn vertrouwelijk van aard. Maar ook publiekelijk poogt het kabinet de kosten voor kwaadwillende actoren te verhogen, bijvoorbeeld door middel van attributieve en/of technische verklaringen of het opleggen van sancties.

Voornoemde leden vinden het daarbij belangrijk om een goede weerbaarheid en cyberverdediging te benadrukken, maar zij vragen hoe het kabinet in dat kader offensieve en defensieve capaciteiten ziet, alsmede het strategische vraagstuk rond spionagepogingen en het al dan niet attribueren van hacks. Ook vragen de aan het woord zijnde leden of er ad hoc is besloten tot de genoemde attributies of dat er beleid ligt om vaker publiekelijk te attribueren?

64. Antwoord van het kabinet

Het kabinet probeert continu het gedrag van kwaadwillende actoren te beïnvloeden. Dat kan via inlichtingenoperaties maar ook via publieke acties zoals sancties en publieke attributies, waarmee landen ter verantwoording kunnen worden geroepen. Voor een verdere beschrijving van de inzet van militaire cybercapaciteiten, zie het antwoord op vraag 11.

Het is cruciaal om continu te werken aan een sterke uitgangspositie ten opzichte van onze tegenstrevers om zo hun handelingsvrijheid binnen aanvaardbare grenzen te houden. Attributie kan daarin kostenverhogend werken. Elke attributie van cyberoperaties aan een staat wordt voorafgegaan door een kabinetsbesluit en wordt gebaseerd op eigen en/of via bondgenoten verkregen inlichtingen.

Responsmaatregelen zoals attributie moeten gewogen worden in de bredere geopolitieke context en het Nederlandse belang. Op basis hiervan en in lijn met de motie Erkens besluit het kabinet, waar mogelijk, tot openbaarmaking van cyberaanvallen door middel van

attributie. Een voorbeeld hiervan is de *Coathanger*-operatie die in februari 2024 door de MIVD werd toegeschreven aan China.[18]

De leden van de SGP-fractie vragen naar de cyberconsultaties met de Verenigde Staten, het Verenigd Koninkrijk, Zuid-Korea, India en Zuid-Afrika.

Kan het kabinet de resultaten hiervan op hoofdlijnen schetsen? De aan het woord zijnde leden zien deze als mogelijk zeer nuttig. Zij zijn benieuwd naar een overzicht van de gemeenschappelijke dreigingen en de sterke kanten en ook nog verbeterpunten in de dialoog met de verschillende landen.

65. Antwoord van het kabinet

Zowel de diplomatieke als de meer operationele betrekkingen van Nederland met de VS en het VK op het gebied van digitale dreigingen zijn hecht en gaan ver terug. Tijdens consultaties met deze landen worden onder andere analyses gedeeld over het dreigingslandschap (vooral gericht op China en Rusland) en over de gezamenlijke aanpak van cyberdreigingen, bijvoorbeeld d.m.v. het delen van inlichtingen of het afstemmen van sanctiebeleid. Bij deze consultaties zijn veel ministeries alsook de AIVD/MIVD en het NCSC betrokken.
Daarnaast voerde Nederland in 2024 en 2025 ook bilaterale cyberdialogen met landen waarmee de relatie zich nog in de opbouwende fase bevindt, zoals Zuid-Korea, India en Zuid-Afrika. Cyberveiligheid, cybercriminaliteit, *internet governance* en multilaterale aangelegenheden zijn onderwerpen die in vrijwel alle bilaterale en regionale dialogen terugkomen. De consultaties met Zuid-Afrika en India stonden primair in het teken van het uitwisselen van kennis en ervaringen. In de relatie met Zuid-Korea is sprake van meer operationele samenwerking.

De leden van de SGP-fractie vragen het kabinet of zij de Tweede Kamer kan informeren over haar besluit om het nieuwe VN-cybercrimeverdrag wel of niet te ratificeren? Kan zij haar standpunt daarover en motivatie uiteenzetten?

66. Antwoord van het kabinet

Momenteel wordt door de Europese Commissie bezien wat de mogelijke juridische gevolgen zijn van ratificatie van dit verdrag ten opzichte van bestaande wet- en regelgeving. Deze eerste analyse zal tevens worden afgezet tegen de bestaande Nederlandse wet- en regelgeving omtrent cybercrime. Aan de hand daarvan zal het kabinet haar positie bepalen ten opzichte van mogelijke ratificatie.

Vragen en opmerkingen van de leden van de ChristenUnie-fractie

De leden van de ChristenUnie-fractie hebben met interesse kennisgenomen van de voortgangsbrief over de uitvoering van de Internationale Cyberstrategie 2023-2028. Zij hebben daarover nog enkele vragen.

[18] MIVD onthult werkwijze Chinese spionage in Nederland | Nieuwsbericht | Defensie.nl

Deze leden zien dat zelfs sinds het verschijnen van de voortgangsbrief er grote verschuivingen op het wereldtoneel hebben plaatsgevonden, die relevant zijn voor de cyberstrategie van Nederland. De leden van de ChristenUnie-fractie lezen in de strategie dat er stappen zijn gezet richting een meer proactieve omgang met cyberdreigingen. Met de huidige verschuivingen op het wereldtoneel lijkt deze houding relevanter dan ooit. Deze leden merken op dat bijvoorbeeld de nadruk meer op investeringen in defensie en Europese samenwerking is komen te liggen.

Welke ontwikkelingen signaleert de minister als het gaat om de cyberstrategie? En welke eventuele extra inzet acht de minister, zowel nationaal als internationaal, noodzakelijk om de huidige digitale dreigingen tegen te gaan?

67. Antwoord van het kabinet

Hiervoor verwijs ik u naar het antwoord op vraag 1.

De leden van de ChristenUnie-fractie steunen de inzet om coalities te bouwen om tegenspel te bieden aan landen met een offensief cyberprogramma gericht tegen onze belangen.

Deze leden vragen of de geopolitieke verschuivingen van de afgelopen maanden impact hebben gehad op deze inzet en of deze tijd ook om andere coalities vraagt?

68. Antwoord van het kabinet

Hiervoor verwijs ik u naar het antwoord op vraag 1

Daarbij denken deze leden voornamelijk aan de samenwerking met de Verenigde Staten. Ervaart de minister een veranderende houding in de samenwerking? In hoeverre is Nederland voor de inzet afhankelijk van de Verenigde Staten en in hoeverre acht de minister het nodig dat Nederland onafhankelijk van de Verenigde Staten te werk gaat in de toekomst wat betreft cybersecurity? Welke inzet zou daarvoor nodig zijn?

69. Antwoord van het kabinet

Hiervoor verwijs ik u naar het antwoord op vraag 50

De minister moest concluderen dat de CTIVD vanwege huisvestingsproblemen en capaciteitsgebrek slechts beperkt toezicht kon houden op de Tijdelijke Wet Cyberoperaties. De leden van de ChristenUnie-fractie vragen de minister of er in de afgelopen maanden verbetering van het toezicht heeft kunnen plaatsvinden? Deze leden vragen de minister wat er gedaan wordt om het capaciteitsgebrek te verminderen of hieraan tegemoet te komen?

70. Antwoord van het kabinet

Hiervoor verwijs ik u naar het antwoord op vraag 8.

Deze leden lezen voorts dat met steun van Nederland de *Global Forum on Cyber Expertise* is opgericht.

Zij zien grote bezuinigingen van dit kabinet op het gebied van ontwikkelingssamenwerking en vragen de minister of deze bezuinigingen op een bepaalde manier impact hebben op de inzet van dit kabinet rondom de derde doelstelling? Zo ja, op welke manier?

71. Antwoord van het kabinet

De inzet van het kabinet op het gebied van het versterken van de cyberweerbaarheid in opkomende landen wordt gefinancierd vanuit de begroting van het ministerie van Buitenlandse Zaken. De bezuinigingen op het ministerie van Buitenlandse Zaken hebben significante impact op de uitvoering van de internationale cyberstrategie. De taakstelling beperkt de beschikbare middelen voor programma's die de cyberweerbaarheid in opkomende landen versterken.
Bezuinigingen op de begroting voor Buitenlandse Handel en Ontwikkelingshulp hebben geen impact op deze doelstelling.

II Antwoord/ Reactie van de minister

III Volledige agenda

- de brief van de minister van Buitenlandse Zaken van 6 december 2024 over de uitvoering van de Internationale Cyberstrategie 2023-2028 (26 643/30 821, nr. 1252).