Internationale Cyberstrategie 2023 - 2028

Daadkrachtige Diplomatie in het Digitale Domein

Inhoudsopgave

Samenvatting

Nederland streeft naar een open, vrij en veilig cyberdomein. Die doelstelling, opgenomen in de eerste Internationale Cyberstrategie uit 2017[1] en in de Nederlandse Cybersecurity-strategie (NLCS)[2] uit 2022, blijft actueel. De geopolitieke en technologische context waarbinnen dit doel wordt nagestreefd, is sinds 2017 echter ingrijpend veranderd.

Door de Russische oorlog tegen Oekraïne wordt Europa weer geconfronteerd met een groot conventioneel conflict. Rusland heeft zich daarmee buiten de internationale orde geplaatst. Ook de gevolgen van China's assertiviteit als economische en militaire mogendheid laten zich voelen. De geopolitieke spanningen die volgen uit deze ontwikkelingen hebben een rechtstreekse uitwerking op de digitale omgeving. Ook daar staan fundamenteel verschillende visies tegenover elkaar waardoor openheid, vrijheid en veiligheid onder steeds grotere druk staan.

Omdat de digitale omgeving, mede door de snelle technologische ontwikkelingen, inmiddels een integraal onderdeel is geworden van onze samenleving, is een effectievere inzet noodzakelijk om onze belangen - ook in die minder tastbare omgeving - te beschermen. De voortdurende cyberaanvallen, gericht tegen onze overheden, bedrijven en burgers veroorzaken niet alleen enorme directe schade, ze bedreigen ook onze strategische nationale belangen.

Parallel hieraan laat de kloof tussen gedigitaliseerde en minder gedigitaliseerde landen zich steeds duidelijker voelen. Een groot aantal landen slaagt er onvoldoende in cyberveiligheid onderdeel te maken van digitaliseringsprocessen en beleid. Dat maakt hen kwetsbaar voor cybercriminelen en statelijke actoren die kwaadwillende cyberoperaties uitvoeren. Daarnaast zorgt deze ontwikkeling ervoor dat burgers in die landen makkelijker doelwit zijn van mensenrechten schendingen online. Tot slot zet het gebrek aan cyberveiligheid een rem op sociaaleconomische ontwikkeling.

Met voorliggende interdepartementale internationale cyberstrategie (ICS) beschrijft het kabinet hoe het de komende jaren wil inspelen op deze internationale ontwikkelingen binnen multilaterale fora zoals de EU en de NAVO maar ook daarbuiten in nieuwe coalities. Deze inzet kan als volgt worden samengevat:

Om de cyberdreiging van staten en criminelen tegen te gaan zal Nederland de middelen waarover het beschikt proactiever, meer geïntegreerd en strategischer inzetten, waar mogelijk met EU-partners en NAVO-bondgenoten. Daarmee streven we naar maximale effectiviteit om statelijke en niet-statelijke dreigingen te adresseren. Het gaat daarbij om middelen als diplomatieke kanalen, sancties, economische drukmiddelen, inlichtingenmatig onderzoek, militaire en justitiële slagkracht en samenwerking met de private sector. Tegelijkertijd zullen de afzonderlijke instrumenten worden versterkt.

Om democratische en mensenrechtelijke principes online te versterken zal Nederland, met verhoogde inzet en in een brede coalitie van landen, onderzoekers, bedrijven en maatschappelijk middenveld, uitwerken hoe internationaal erkende principes in de digitale ruimte moeten worden toegepast ter bevordering van de mondiale cyberveiligheid. Cyberveiligheid en mensenrechten zijn complementair en versterken elkaar. Individuele veiligheid is een kerncomponent van cyberbeveiliging en een open, vrij en veilig internet is een cruciaal uitgangspunt bij het bevorderen van online mensenrechten. Nederland stimuleert daarnaast staten en bedrijven om (onbedoelde) schendingen van online mensenrechten tegen te gaan. Ook zet Nederland in op waarborging van mensenrechten en democratische beginselen bij de ontwikkeling van standaarden voor nieuwe technologieën en online diensten.

Om een wereldwijd open, vrij en veilig internet te behouden zal Nederland de publieke kern - oftewel de technische laag - van het internet beschermen, onder andere om fragmentatie tegen te gaan. Fragmentatie *op* het internet is in zeker zin al een gegeven. Voor de technische laag van het internet echter, moet dit te allen tijde voorkomen worden. Daarbij zal Nederland de betrokkenheid van opkomende landen bij het beheer van het internet bevorderen en expertise delen om de cybercapaciteiten van deze landen verder te versterken zodat ook zij de vruchten van een veilige digitale omgeving kunnen plukken.

[1] Kamerstuk 26 643 nr. 447
[2] Nederlandse Cybersecuritystrategie 2022 – 2028, oktober 2022

Inleiding

Opzet Internationale Cyberstrategie

Deze ICS beschrijft de interdepartementale inzet voor de komende vijf jaar (2023 – 2028). Een analyse van de belangrijkste ontwikkelingen in het digitale domein, is te vinden in hoofdstuk 1 (Mondiale ontwikkelingen in het digitale domein). In hoofdstuk 2 wordt toegelicht hoe die ontwikkelingen zich vertalen naar drie beleidsdoelstellingen en welke instrumenten worden ingezet om die doelstellingen te realiseren. Aan het slot van de strategie treft de lezer een niet-uitputtend overzicht van concrete acties, geïdentificeerd om invulling te geven aan de resultaatgebieden. Daarbij is aangegeven welke betrokken departementen en instanties primair verantwoordelijk zijn voor de uitvoering van de acties. Dit overzicht bouwt voort op het actieplan behorend bij de NLCS[3]. Het overzicht wordt in de aankomende jaren regelmatig geactualiseerd.

Voorwaarden voor effectieve implementatie van het internationaal cyberbeleid

In de competitie om strategische politieke en economische belangen die in het cyberdomein plaatsvindt, kan Nederland – in internationale coalities - alleen effectief opereren indien de internationale cyberinzet wordt geïntegreerd in het bredere buitenlandbeleid. Het vergroten van onze cyberveiligheid en die van derde landen is niet slechts een technisch onderwerp dat geïsoleerd kan worden bezien. Het is zaak het internationaal cyberbeleid te koppelen aan relevante buitenlandpolitieke thema's zoals (economische) veiligheid, mensenrechten, rechtsstaat en multilateralisme, maar ook aan de bredere inzet binnen de EU, NAVO, OVSE en VN. In dat licht moeten cybervraagstukken regelmatiger onderdeel uitmaken van diplomatieke inzet zoals officiële veiligheids- of politieke consultaties met derde landen en aan de orde moeten komen tijdens bijeenkomsten van de Raad van de Europese Unie zoals de Raad Buitenlandse Zaken (inclusief Defensie en Ontwikkelingssamenwerking) maar ook tijdens de Raad Concurrentievermogen.

Evenzo moet de verbinding worden gelegd tussen het internationaal cyberbeleid en de agenda voor Buitenlandse Handel en Ontwikkelingssamenwerking (BHOS). Cyberveiligheid, in de zin van het beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatiesystemen, is een van de voorwaarden voor een stabiele samenleving, duurzame en toekomstgerichte ontwikkeling van de economie, en veiligheid van de gebruiker in opkomende landen. Gebrekkige cyberveiligheid ver weg kan bovendien gevolgen hebben voor de cyberveiligheid dichtbij. Daarom is het zaak om binnen de BHOS-inzet gericht op het vergroten van digitalisering vanaf de start aandacht te besteden aan onderhoud en veiligheid van de ICT-oplossing. Bijdragen aan het dichten van de 'kloof' met minder gedigitaliseerde landen is daarbij een centraal aandachtspunt.

Om in te kunnen spelen op relevante cyberontwikkelingen in derde landen is het ook van belang dat de cyberkennis en -capaciteit van Nederlandse vertegenwoordigingen in het buitenland verder wordt versterkt. Het amendement Mulder stelde het ministerie van Buitenlandse Zaken in staat het aantal cyberdiplomaten op ambassades aanzienlijk uit te breiden.[4] Daardoor heeft een toenemend aantal functies op 34 ambassades en Permanente Vertegenwoordigingen inmiddels een significante cybercomponent. Die intensivering werpt zijn vruchten af. Zo is Nederland met aanzienlijk meer landen in dialoog en wordt Nederland regelmatig benaderd om kennis en expertise te delen in multilaterale werkgroepen en tijdens cyberconferenties. Nederland heeft zijn profiel als relevante cyberactor door middel van de diplomatieke inzet van cyberdiplomaten, alsook van de Nederlandse cyberambassadeur, in veel landen versterkt. Die inzet leidt ook tot intensievere lokale samenwerking met attachés van bijvoorbeeld de ministeries van EZK, Defensie, BZK en Justitie en Veiligheid. De noodzaak voor verdere ontwikkeling van cyberkennis en expertise geldt ook voor de departementen in Den Haag. We behouden zoveel mogelijk de bestaande cyberkennis binnen departementen en organisaties en trekken zo nodig externe expertise aan.

[3] Actieplan Nederlandse Cybersecuritystrategie 2022 - 2023 | Publicatie | Rijksoverheid.nl

[4] Vaststelling van de begrotingsstaat van het Ministerie van Buitenlandse Zaken (V) voor het jaar 2022 | Tweede Kamer der Staten-Generaal

Mondiale ontwikkelingen in het cyberdomein

Digitalisering is de afgelopen decennia de motor onder onze ontwikkeling geweest. Het heeft veel landen in staat gesteld hun economieën en maatschappelijke sectoren zoals de zorg, transport en energie versneld te ontwikkelen. De vruchten van digitalisering zullen we, zeker met de opkomst van nieuwe digitale technologieën zoals kunstmatige intelligentie (AI) en quantumtechnologie, ook in de toekomst kunnen blijven plukken. Digitalisering heeft gezorgd voor toenemende mondiale verwevenheid en heeft de barrières voor betrekkingen tussen landen verlaagd. In tijden van geopolitieke stabiliteit zijn de risico's van die intensievere onderlinge verbinding beheersbaar. In tijden van geopolitieke onrust, leidt deze digitale verwevenheid echter tot grote uitdagingen. Bovendien heeft exponentiele digitalisering zowel de mogelijkheden als het aanvalsoppervlak voor kwaadwillende actoren vergroot, en die dreiging zal in de toekomst met de doorontwikkeling van digitale technologieën alleen maar toenemen.

De geopolitieke dynamiek die zich in de fysieke wereld ontvouwt, vertaalt zich ook naar de digitale omgeving. Onze nationale veiligheid, ons verdienvermogen en de veilige online omgeving van de burger worden op dagelijkse basis bedreigd door statelijke en criminele actoren. Net als de fysieke wereld is ook de digitale wereld inmiddels het speelveld van strategische competitie, waarin conflicterende belangen en waarden in toenemende mate tot confrontaties leiden. In de digitale omgeving komt deze competitie vooral tot uiting via cyberoperaties - om te spioneren, te saboteren en desinformatie te verspreiden.

Deze dynamiek wordt versterkt door snelle technologische ontwikkelingen. Er is sprake van een proliferatie aan dreigingen door staten en cybercriminelen dankzij de grotere toegankelijkheid en relatief lage kosten van cyberinstrumenten en de toepassing van nieuwe digitale technologieën bij cyberoperaties. Nieuwe en goedkopere cybermiddelen worden niet alleen ingezet voor buitenlandse cyberoperaties of spionage, maar maken het ook makkelijker om de eigen bevolking (advocaten, politici, mensenrechtenverdedigers, journalisten) te hacken en online te bedreigen en vervolgen. Ook wordt steeds vaker de valse dichotomie tussen cyberveiligheid en mensenrechten gebezigd. Zo worden internet *shutdowns* vaak gerechtvaardigd als kwesties van nationale veiligheid.

De opkomst en verdere ontwikkeling van technologieën werpt ook vragen op over het beheer van het internet en de ontwikkeling van standaarden voor nieuwe technologieën. Lange tijd werden discussies over technische standaarden voor nieuwe technologieën alsook discussies over het beheer van het internet gekenmerkt door betekenisvolle betrokkenheid van zowel statelijke als niet-statelijke belanghebbenden. In de huidige geopolitieke context staat dat "multistakeholder-model" echter onder druk. Door verschillende staten wordt gepoogd technische discussies te *multilateraliseren* waardoor betrokkenheid van maatschappelijke organisaties, de private sector, academici en de technische gemeenschap onder druk komt te staan. Dat heeft ook gevolgen voor het model voor het beheer van het internet (*internet governance*).

Voor het effectief en geïntegreerd adresseren van deze brede en complexe uitdagingen is een handelingsbekwame Europese Unie een voorwaarde. In Europees verband zijn al belangrijke stappen gezet op het gebied van wet- en regelgeving om burgers en bedrijven beter te beschermen tegen statelijke en niet-statelijke cyberdreigingen, bijvoorbeeld via de Netwerk- en Informatiebeveiliging richtlijn (NIB2) en de wet inzake digitale diensten (DSA). Tegelijkertijd kan de vraag worden gesteld of de Unie op buitenlandpolitiek terrein niet nog beter moet worden toegerust om effectief deel te kunnen nemen aan de strategische competitie die zich steeds scherper aftekent in de digitale omgeving. Daartoe lijkt het noodzakelijk het gedeelde gevoel van urgentie onder lidstaten en EU-instellingen, over de strategische cyberdreiging die uitgaat van een aantal staten, verder te versterken. Ook is het van belang om technologische ontwikkelingen nog meer door een geopolitieke lens te bekijken door de verbinding te versterken tussen de interne wet- en regelgevings-trajecten en het Europese externe cyberbeleid.

De multipolaire wereld heeft ook tot gevolg dat het enkel in stand houden van bestaande coalities en partnerschappen - zoals de EU, NAVO en het trans-Atlantisch partnerschap - niet langer volstaat om onze belangen in het cyberdomein adequaat te kunnen verdedigen. Cyberveiligheid en de inrichting van het cyberdomein zijn per definitie grensoverschrijdende vraagstukken. Daarmee groeit het belang van nieuwe partnerschappen. Het dient de Nederlandse

strategische belangen als landen waarmee wij politieke en economische betrekkingen onderhouden weerbaarder worden tegen externe cyberdreigingen en de eigen soevereine belangen in het cyberdomein zelf beter kunnen verdedigen.

In deze context zien we ook dat het relatieve gewicht van opkomende en ontwikkelingslanden in multilaterale cyberdiscussies steeds groter wordt, bijvoorbeeld over de toepasbaarheid van internationaal recht in het cyberdomein en de gezamenlijke aanpak van cybercriminaliteit. In het aanhalen van de banden met nieuwe partners is het zaak een balans te vinden tussen enerzijds de stip op de horizon van een open, vrij en veilig cyberdomein, en anderzijds het behartigen van directe eigenbelangen in een complexe realiteit waarin niet alle landen waarmee we samenwerken onze waarden en principes volledig onderschrijven.

Doelstellingen

Overkoepelende doelstelling van het Nederlandse internationale cyberbeleid:

Het kabinet streeft naar een open, vrij en veilig cyberdomein waarin staten zich verantwoord gedragen, universele mensenrechten en rechtsstaatprincipes worden gegarandeerd, toepasselijkheid van het internationaal recht wordt erkend en het decentrale en open karakter van het internet behouden blijft.

Geopolitieke ontwikkelingen maken de omstandigheden voor verwezenlijking van deze doelstelling zeer complex. Machtsverschuivingen en toegenomen spanningen, in combinatie met snelle technologische ontwikkelingen, leiden tot toenemende *geopolitisering* van het cyberdomein. Deze ontwikkelingen vertalen zich naar een **drietal prioritaire uitdagingen** voor de komende jaren:

Cyberoperaties die in toenemende mate worden ingezet om strategisch politieke, economische en militaire doelstellingen te bereiken, zetten onze veiligheid en welvaart onder druk.

Denk aan politieke en economische spionage, desinformatie en (voorbereidingen voor) sabotage.

Democratische en mensenrechtelijke principes online staan onder toenemende druk.

Steeds meer regimes gebruiken digitale technologieën om de eigen positie te verstevigen en burgers, het maatschappelijk middenveld en oppositie te controleren. Denk aan inzet van surveillancetechnologie en internet shutdowns.

Verdere politisering van internationale technische organisaties.

Staten proberen hun invloed op de vormgeving van standaarden voor nieuwe technologieën alsook op de inrichting van het internet te vergroten door inspraak van de private sector, maatschappelijke organisaties en academici te beperken.

Op basis van deze uitdagingen, komt het kabinet tot een **drietal doelstellingen** in de periode 2023 – 2028

1. *Tegengaan van cyberdreigingen van staten en criminelen*
2. *Versterken van democratische en mensenrechtelijke principes online*
3. *Behoud van een wereldwijd verbonden, open, vrij en veilig internet.*

Om deze doelstellingen te verwezenlijken is naast de geïdentificeerde resultaatgebieden en concrete activiteiten een aantal **doorsnijdende beleidsinstrumenten** relevant. Zij vormen een rode draad door het internationaal cyberbeleid voor de aankomende vijf jaar:

- Vergroten van de rol van de EU en NAVO als internationale cyberactoren.
- Multilateralisme als instrument om te komen tot verantwoord gedrag in het cyberdomein.
- Versterken van bestaande en bouwen van nieuwe coalities met opkomende landen.
- Investeren in inlichtingencapaciteiten.
- Actief betrekken van de cybergemeenschap (private sector, maatschappelijke organisaties en academici) bij cybervraagstukken.
- Diplomatiek netwerk versterken en technische en beleidsmatige cyberkennis vergroten.

Strategische doelstelling 1

Tegengaan van cyberdreigingen van staten en criminelen

Resultaatgebieden
- Van reactieve naar proactieve omgang met cyberdreigingen
- Vergroten van het zicht op de dreiging
- Versterkte slagkracht in het cyberdomein
- Slagvaardige internationale coalities
- Versterking en bestendiging van normen voor verantwoord statelijk gedrag
- Versterkte internationale samenwerking tegen cybercriminaliteit

Analyse

In lijn met de eerder omschreven geopolitieke ontwikkelingen zien we dat staten de digitale ruimte structureel én intensief gebruiken voor de behartiging van hun belangen. Cyberoperaties, bijvoorbeeld voor het vergaren van politieke en economische inlichtingen, beïnvloeding en sabotage zijn daartoe belangrijke instrumenten: ze zijn relatief goedkoop en schaalbaar en ze hebben een hoge, vaak langdurige opbrengst. De cyberoperaties blijven veelal onder de juridische drempel van een gewapend conflict. Echter, de effecten die met de optelsom van de vele afzonderlijke cyberoperaties kunnen worden bereikt, benaderen de effecten die met gewapend conflict kunnen worden bereikt. Temeer doordat cyberoperaties in samenhang worden uitgevoerd met middelen buiten het cyberdomein, zoals in hybride campagnes. Naast de cyberdreiging die uitgaat van statelijke actoren is cyber criminaliteit (mogelijk uitgevoerd met steun van of gefaciliteerd door staten) uitgegroeid tot een dreiging die de nationale veiligheid kan raken.

Om statelijk gedrag in het cyberdomein te begrenzen en de kans op conflicten te verkleinen, is in de afgelopen jaren met name in VN-verband intensief onderhandeld over internationale afspraken waaraan staten zich in het cyberdomein zouden moeten houden. Tegelijkertijd is gewerkt aan afspraken over de internationale aanpak van cybercriminaliteit. Nederland heeft in deze onderhandelingen een actieve rol gespeeld. In de huidige geopolitieke context lijken de mogelijkheden voor verdere consensusafspraken over normen in het cyberdomein en over het tegengaan cybercriminaliteit binnen de VN echter beperkt.

Rusland en China, gesteund door enkele partners, lijken bereid het bestaande normatief kader te ondermijnen. Zij profileren zich ook in VN-verband met een agenda gericht op het beperken van ruimte voor tegengeluid in de digitale omgeving. Deze landen verzetten zich ook tegen de deelname van niet-statelijke actoren (maatschappelijke organisaties, private sector, academici en de technische gemeenschap) aan discussies over het cyberdomein binnen de VN. Zij pleiten daarnaast voor een juridisch bindend verdrag voor verantwoord statelijk gedrag in het digitale domein. Voor Nederland en gelijkgezinde landen is dat prematuur. De VN heeft namelijk bij consensus bepaald dat bestaand internationaal recht, inclusief mensenrechten en het humanitair oorlogsrecht, integraal van toepassing is op het digitale domein. Nederland en gelijkgezinde landen zijn van mening dat eerst gesproken moet worden over de vraag hoe die toepassing in de praktijk precies moet worden georganiseerd, om zo het bestaande normatieve kader te versterken en implementatie ervan te bevorderen. Alleen op basis van deze inhoudelijke discussies kan vervolgens worden bepaald of nieuw internationaal recht noodzakelijk is.

Tot slot is het belangrijk op te merken dat door de razendsnelle wereldwijde digitalisering en de toegenomen cyberdreigingen die uitgaan van statelijke en niet-statelijke actoren, de interesse van VN-lidstaten uit alle regio's in internationaal cybersecuritybeleid toeneemt. Opkomende landen zullen de komende jaren een groeiende rol spelen in het vormgeven van de toekomst van het cyberdomein. Net als op andere geopolitieke onderwerpen willen veel van

deze landen zich niet laten dwingen een keuze te maken tussen de concurrerende geopolitieke blokken binnen de VN. Veel van deze landen hebben bovendien onvoldoende capaciteit om cyberdreigingen te identificeren en te adresseren. Hierdoor worden zij kwetsbaar voor beïnvloeding, inmenging en ongewenste afhankelijkheden.

Probleemstelling

De geopolitieke strijd in het cyberdomein gaat samen met een toenemend belang van dit domein voor de Nederlandse veiligheid, economie en welvaart.
Hierdoor is de cyberdreiging waarmee we worden geconfronteerd aanzienlijk gegroeid. Het versterken van normen voor verantwoord gedrag van staten in het cyberdomein en het formuleren van reacties op overtredingen van deze normen zijn in deze context nog steeds belangrijk maar die inzet is niet voldoende om onze nationale belangen effectief te beschermen.

Antwoord

Van reactieve naar proactieve en strategische omgang met cyberdreigingen

In reactie op de grotere cyberdreiging zullen we het volledige spectrum van instrumenten waarover we beschikken om Nederlandse belangen in het cyberdomein veilig te stellen proactiever, meer geïntegreerd en strategischer moeten inzetten, waar mogelijk met EU-partners en NAVO-bondgenoten. Daarmee streven we naar maximale effectiviteit om statelijke en niet-statelijke dreigingen te adresseren. Het gaat daarbij om middelen als diplomatieke kanalen, sancties, economische drukmiddelen, inlichtingenmatig onderzoek, militaire en justitiële slagkracht en samenwerking met de private sector. Tegelijkertijd zullen de afzonderlijke instrumenten worden versterkt.

Om de beoogde proactievere en strategischere benadering vorm te geven is intensievere en gerichtere samenwerking tussen alle nationale partners, in - en buiten - het cyberdomein noodzakelijk. Daarbij zal worden voortgebouwd op het interdepartementale cyber responskader, dat sinds 2018 wordt gebruikt en zo nodig zullen aanvullende modellen worden ingericht om informatiedeling en besluitvorming te faciliteren. Tevens zal aansluiting worden gezocht bij relevante trajecten zoals het Rijksbreed responskader statelijke dreigingen. Bijzondere aandacht zal de komende jaren uitgaan naar samenwerking met de private sector, die een steeds belangrijke rol speelt in het tegengaan van cyberdreigingen.

Nederland heeft de afgelopen jaren een voortrekkersrol gespeeld in het vormgeven van internationale diplomatieke reacties op cyberdreigingen en het kabinet beoogt eenzelfde voortrekkersrol in het vormgeven van de proactievere internationale benadering van cyberdreigingen.
Het ministerie van Buitenlandse Zaken zal deze nieuwe benadering, in nauwe samenwerking met alle relevante overheidspartijen, in de komende jaren verder uitwerken.

Naast de proactievere inzet van de middelen die we hebben om onze belangen in het cyberdomein te beschermen, zullen de afzonderlijke instrumenten moeten worden versterkt. In de volgende paragrafen zal daar nader op worden ingegaan.

Een scherper zicht op cyberdreigingen

Aan de basis van een strategischere, pro-actievere aanpak van de dreiging in het cyberdomein, ligt een scherp zicht op die dreiging. Het kabinet investeert daarom fors in de onderzoekscapaciteit van de Inlichtingen- en Veiligheidsdiensten ten behoeve van inlichtingenmatig-diepte-onderzoek[5]. Daarnaast heeft het ministerie van Defensie in de Defensienota 2022 toegezegd vaker informatie over (hybride) dreigingen te delen als dat bondgenoten en partners (NAVO en EU) en de Nederlandse samenleving helpt om zich beter tegen deze dreiging te kunnen beschermen.

Versterkte slagkracht in het cyberdomein

Om assertiever te kunnen optreden is slagkracht in het cyberdomein een voorwaarde. Om die reden versterkt het ministerie van Defensie gericht zijn gevechtskracht in het cyberdomein, onder meer door middel van versterkte informatie-uitwisseling en verhoging van de weerbaarheid, zoals ook bepaald in artikel 3 van het NAVO-verdrag.
Dit draagt bij aan het beperken van digitale dreigingen. Daarnaast zal het kabinet, binnen de juridische kaders, nog meer dan nu de mogelijkheden benutten om kwaadwillende actoren en hun facilitators (digitaal) op te sporen, aan te pakken, te verstoren en te vervolgen.

Op 2 december 2022 heeft het kabinet het wetsvoorstel Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma aangeboden aan de Tweede Kamer. Dit wetsvoorstel is opgesteld naar aanleiding van operationele knelpunten die de AIVD en de MIVD ervaren in onderzoeken naar cyberdreigingen van statelijke actoren. Het wetsvoorstel beoogt de diensten, met behoud van waarborgen, in staat te stellen hun bevoegdheden sneller en effectiever in te kunnen zetten in het digitale domein.

Defensie trekt cyber expertise aan om de offensieve en defensieve cybercapaciteiten uit te breiden. Tevens wordt de *cyber readiness* van Defensie verhoogd door een betere (cyber) inlichtingenpositie te creëren en de digitale weerbaarheid van eenheden en systemen te vergroten. Tot slot wordt de samenwerking met internationale veiligheidspartners verstevigd om bijvoorbeeld hybride dreigingen met vereende krachten het hoofd te bieden. De subtitel van de

[5] Zie Acties met prioriteit pijler III en de financiële onderbouwing in de NLCS okt. 2022

Defensienota 2022 leest om die reden ook 'Investeren in een krachtige NAVO en EU'.

Slagvaardige internationale coalities

Om krachtig tegenspel te bieden aan landen met een offensief cyberprogramma, gericht tegen Nederlandse belangen, zijn sterke coalities een voorwaarde. Zowel in Europees en NAVO-verband als daarbuiten verbeteren we daarom de effectiviteit van bestaande instrumenten en ontwikkelen we nieuwe strategieën om weerbaarheid en slagkracht te optimaliseren.

De EU *cyber diplomacy toolbox* – het geheel aan Europese handelingsopties om op te treden tegen kwaadwillende statelijke cyberactoren – moet beter aansluiten bij de geopolitieke realiteit. Nu is het alleen mogelijk om sancties op te leggen aan personen en entiteiten, terwijl de cyberdreiging van statelijke of aan staten-gelieerde actoren alleen maar toeneemt. Het kabinet pleit er dan ook voor dat het EU cyber sanctieregime vaker wordt ingezet en dat verdergaande sancties mogelijk moeten worden. Ook zou het cybersanctie-instrumentarium landenspecifieker moeten kunnen worden ingezet.

Binnen de EU is het daarnaast belangrijk verbinding te zoeken met andere instrumenten (zoals de *Hybrid Toolbox* en de *Foreign Information Manipulation and Interference Toolbox*) die kunnen worden ingezet om hybride dreigingen door statelijke actoren tegen te gaan. De verschillende toolboxen zijn zelfstandige instrumenten maar een versterkte verbinding maakt het mogelijk effectiever op te treden en versnippering tegen te gaan.

Daarnaast is nauwere EU-NAVO samenwerking nodig om cyberdreigingen het hoofd te bieden. Hier wordt gezocht naar kansen om de EU en NAVO activiteiten elkaar te laten versterken, passend binnen hun respectievelijke competenties, zonder dat ze onnodige duplicatie veroorzaken. Dit gebeurt bijvoorbeeld door synergie te zoeken tussen de *EU cyber diplomacy toolbox* en de *NATO Guide* inzake diplomatieke respons bij cyberincidenten, gezamenlijke cyberoefeningen te organiseren en door middel van praktische samenwerking op werkniveau en capaciteitsopbouw rondom thema's als cyberveiligheid.

Tot slot zal de samenwerking met landen buiten de EU en NAVO verder worden verkend en verdiept. Landen als Japan, Zuid-Korea, Australië en Singapore hebben te maken met een vergelijkbare cyberdreiging als Nederland en investeren ook in hun capaciteiten die dreiging te kunnen adresseren.

Veel andere landen beschikken nog over onvoldoende capaciteit om cyberdreigingen uitgaande van staten en cybercriminelen te identificeren en te adresseren.
Het kabinet versterkt daarom de samenwerking met partners op de Westelijke Balkan, onder andere vanwege de aanhoudende dreiging vanuit Rusland waarmee die landen te maken hebben, maar ook in zuidelijk Afrika, Azië en Oceanië. Veel landen in die regio's ontwikkelen zich snel maar zijn daardoor ook dankbaar doelwit van cyberaanvallen en cybercriminaliteit. Deze landen spelen ook een steeds prominentere rol in de geostrategische competitie die in het cyberdomein plaatsvindt. Nederlandse betrokkenheid helpt die landen hun cyberveiligheid te vergroten én poogt hun betrokkenheid te vergroten bij multilaterale discussies over verantwoord statelijk gedrag en het tegengaan van cybercriminaliteit. Daarbij zoeken we de aansluiting met de Nederlandse en Europese *Indo-Pacific* Strategie, de Afrika-strategie, en het *Global Gateway* programma van de EU. De VN biedt een belangrijk platform om nieuwe contacten te leggen. Ook middels bilaterale en regionale cyberconsultaties wordt verkend op welke wijze Nederland met deze landen verder kan samenwerken, waarbij gedeeld belang het uitgangspunt is.

Versterking en bestendiging van normen voor verantwoord statelijk gedrag

Nederland heeft, als gedigitaliseerd land met een open economie, veel baat bij handhaving van de internationale rechtsorde en multilaterale afspraken in het digitale domein. Bovendien dienen multilaterale afspraken als uitgangspunt om statelijke actoren te kunnen aanspreken op kwaadwillend gedrag. Om die reden zal Nederland in de komende jaren actief blijven bijdragen aan de verdere ontwikkeling en bestendiging van het normatief kader voor verantwoord statelijk gedrag dat de VN-leden op basis van consensus afspraken hebben ontwikkeld. Het normatief kader bestaat onder andere uit de erkenning dat het internationaal recht van toepassing is in het cyberdomein, elf niet-bindende gedragsnormen en praktische maatregelen om escalatie te voorkomen. Daarbij legt het kabinet prioriteit bij de bescherming van de publieke kern van het internet en het stimuleren van discussies over de risico's van nieuwe technologieën, zoals kunstmatige intelligentie, voor internationale cyberveiligheid. Ook moedigt Nederland landen aan zich te houden aan de afspraak al het mogelijke te doen om op te treden tegen cyberactiviteiten komende van hun grondgebied. De ervaringen die Nederland op doet in VN-discussies over verantwoord statelijk gedrag in het cyberdomein zijn daarnaast ook relevant voor discussies over nieuwe aanverwante beleidsthema's waarop multilaterale afspraken nodig zijn, zoals ruimtevaart en militair gebruik van AI.

Binnen de VN zet het kabinet in het bijzonder in op de ontwikkeling van de relatie met opkomende en ontwikkelingslanden. Bijzondere aandacht gaat daarbij uit naar belangrijke regionale spelers. Belangrijke doelstelling van de VN-discussies is dat uiteindelijk alle landen in staat worden gesteld om de gemaakte afspraken te implemente-

ren.
Om zowel verdere ontwikkeling als implementatie van het normatief kader verder te brengen steunt Nederland het Frans-Egyptische initiatief tot een *UN Programme of Action to advance responsible State behaviour in cyberspace* (PoA).

Tot slot werkt Nederland in samenwerking met een aantal partnerlanden aan het vergroten van de deelname van vrouwelijke vertegenwoordigers in VN-processen via het *Women in Cyber-fellowship*. Middels dit programma is het aantal vrouwen alsook het aantal actief deelnemende landen in VN-onderhandelingen aanzienlijk verhoogd. Het kabinet zet in op continuering en uitbreiding van dit programma.

Versterkte internationale samenwerking tegen cybercriminaliteit

Om tegenwicht te bieden aan de wereldwijde toename van schade die wordt geleden door cybercriminaliteit richt de Nederlandse inzet zich op een aantal sporen. De Nederlandse diplomatieke inzet inzake het tegengaan van cybercriminaliteit richt zich primair op het bestrijden van vrijhavens voor cyber-criminele groeperingen conform het VN-normatief kader en het cybercrimeverdrag, oftewel het verdrag van Boedapest, van de Raad van Europa. Daarnaast neemt Nederland deel aan de onderhandelingen over een VN-verdrag inzake cybercriminaliteit. Van belang is dat dit verdrag de internationale aanpak tegen cybercriminaliteit versterkt, maar niet misbruikt kan worden om mensenrechten online in te perken, zoals het recht op vrijheid van meningsuiting. Daarop speelt Nederland, binnen EU-verband, een aanjagende rol. Ook assisteren we landen bij de bestrijding van cybercriminaliteit bijvoorbeeld bij het opstellen of harmoniseren van wetgeving in lijn met het Boedapest verdrag.

Bij de bestrijding van cybercriminaliteit, van preventie tot respons en van opsporing tot vervolging en verstoring, werkt het kabinet intensief samen met landen binnen en buiten de EU. Deze samenwerking ziet onder andere op het verlenen van rechtshulp in strafzaken. Tevens zet het kabinet in op versterking van internationale informatie-uitwisseling over de ontwikkeling van cybercriminaliteits-dreigingen. Het kabinet wil het internationale bewustzijn en gedeeld begrip over deze dreigingen en het bestrijden ervan in internationaal verband vergroten, in het bijzonder ten aanzien van *ransomware*. Nederland is een actief lid van het internationale *Counter Ransomware Initiative*, een Amerikaans initiatief waarin met een grote groep landen ervaringen worden uitgewisseld over bijvoorbeeld weerbaarheid, verstoring van *ransomware*-groeperingen, publiek-private samenwerking en diplomatieke inzet.

De mensenrechtendimensie van de aanpak van cybercriminaliteit, inclusief stevige waarborgen, verdient wat het kabinet betreft bijzondere aandacht. Internationale afspraken over opsporing en vervolging hebben potentieel grote impact op de rechten van individuen en bepaalde groepen in de samenleving zoals minderheden, politiek opponenten, journalisten en de LHBTIQ+ gemeenschap. Zeker nu technologische ontwikkelingen leiden tot een exponentiële groei van opsporingsmiddelen die ingezet kunnen worden voor repressieve doeleinden. Ook met verschillende landen buiten de EU zoals de VS, Japan en Canada wordt de Nederlandse expertise hierop gedeeld.

Inzet op verhoging digitale weerbaarheid in EU-verband

Het kabinet benut actief de kansen die samenwerking binnen de Europese Unie biedt om de digitale weerbaarheid op EU-niveau te verhogen. Nederland neemt het voortouw in de samenwerking tussen EU-lidstaten en draagt op deze manier bij aan een digitaal weerbare Unie. Hiermee worden digitale risico's van grensoverschrijdende aard aangepakt en wordt een gecoördineerde reactie gegeven op grootschalige cyberincidenten en -crises binnen en buiten de EU.

In EU-verband blijft het kabinet zich daarom actief inzetten voor het maken van goede afspraken en blijft het bijdragen aan (aankomende) EU-voorstellen en wetgeving ten behoeve van het verhogen van de digitale weerbaarheid. Nederland neemt daarnaast actief deel aan EU-brede crisisoefeningen. In de Nederlandse Cybersecurity Strategie 2022-2028 wordt nader ingegaan op verschillende belangrijke EU-initiatieven waaraan het kabinet bijdraagt ten aanzien van het vergroten van de digitale weerbaarheid, zoals de Netwerk en Informatiebeveiligingsrichtlijn (NIB2) en de recent verschenen Cyber Resilience Act.

Strategische doelstelling 2

Versterken van democratische en mensenrechtelijke principes online

Resultaatgebieden
- Strategische coalities voor erkenning en toepassing van internationaal recht en mensenrechten online
- Stimuleren van staten en bedrijven om online mensenrechtenschendingen tegen te gaan
- Waarborging van mensenrechten en democratische beginselen bij standaarden voor nieuwe technologieën

Analyse

In de twaalf jaar dat de organisatie *Freedom House* wereldwijd internetvrijheid in kaart heeft gebracht, is deze drastisch ingeperkt. Zo is het aantal keren dat het internet door overheden werd afgesloten de afgelopen jaren gestegen.[6]
In een toenemend aantal landen wordt in tijden van politieke onrust of crisis het internet - of specifieke diensten op het internet zoals Twitter - geblokkeerd voor gebruikers; vaak met als doel om onderlinge communicatie te verhinderen of te voorkomen dat informatie over het geblokkeerde gebied naar buiten komt. Volgens het kabinet vormt toegang tot online media en diensten een essentieel onderdeel van mediavrijheid en vrijheid van meningsuiting. Zorgwekkend is dat deze blokkades vaak samengaan met andere mensenrechtenschendingen; een recent voorbeeld hiervan is dat na de internet *shutdown* in Belarus het politiegeweld tegen de deelnemers aan protesten toenam. De VN rapporteerde dat ook in Myanmar internet beperkingen worden gebruikt om mensenrechtenschendingen te verbergen.[7] Zonder internet worden journalisten, mensenrechtenverdedigers en humanitaire organisaties tegengewerkt om bewijs te verzamelen en hierover te rapporteren.

Content op het internet

Naast het beperken van de toegang tot internet richten overheden in veel landen zich ook op de inhoud op het internet (ook wel *content* genoemd) om dissonante of gemarginaliseerde stemmen te smoren. Zo wordt wetgeving gericht op "cyberveiligheid" vaak misbruikt om kritiek op de regering in brede zin online te verbieden, of is strenge regelgeving van kracht voor contentmoderatie waarbij autoriteiten bepaalde onwelgevallige berichten van de internet-platformen laten verwijderen, als voorwaarde voor toegang van deze platformen tot landelijke netwerken.
Het tegengaan van desinformatie en haatspraak wordt door veel staten gebruikt als voorwendsel om censuur te plegen[8].

Anderzijds wordt content gebruikt als instrument om discussies in het online publieke domein te beïnvloeden. Desinformatie wordt ingezet om de oorlog in Oekraïne te rechtvaardigen. Haatspraak en extremisme worden toegestaan om bijvoorbeeld vrouwen (in het bijzonder parlementariërs), politieke opponenten of gemarginaliseerde groepen zodanig te intimideren dat zij zich uit het publieke debat terugtrekken. De internationale gemeenschap staat de komende jaren voor de uitdaging om een balans te vinden tussen het tegengaan van dit soort schadelijke desinformatie, haatspraak en propaganda, en tegelijkertijd het bewerkstelligen van een vrij en pluriform online medialandschap.

Technologische surveillance

Verregaande digitale ontwikkelingen, in bijvoorbeeld kunstmatige intelligentie, vergroten de effectiviteit van bestaande technologieën en toepassingen. Dat geldt ook voor toepassingen die digitale surveillance mogelijk maken. Voorbeelden van deze toepassingen zijn gezichtsherkennings-

[6] Op 1 maart 2023 publiceerde Access Now het rapport dat er in 2022 het meeste shutdowns ooit plaatsvonden; 187 keer in 35 verschillende landen. Access Now #KeepIt On report 2022: https://www.accessnow.org/internet-shutdowns-2022/
[7] VN Persbericht van 7 juni 2022: Myanmar: UN experts condemn military's "digital dictatorship" https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship
[8] Zie onder andere het rapport van de speciale rapporteur van de Verenigde Naties voor de bevordering en bescherming van het recht op vrijheid van mening en meningsuiting: "Disinformation and freedom of opinion and expression"

technologie, big-data analyse en software die gebruikt worden voor het binnendringen van bijvoorbeeld telefoons. Daar waar deze technologie rechtmatig ingezet wordt kan dit een cruciaal instrument zijn in bijvoorbeeld misdaadbestrijding. Maar dit soort technologieën kan ook worden misbruikt voor politieke controle of het onderdrukken van de oppositie waarmee universele mensenrechten worden geschonden. Helaas zijn er veel internationaal voorbeelden te vinden waar deze technologie onrechtmatig is ingezet tegen advocaten, politici, mensenrechtenverdedigers, diplomaten of journalisten.

Ontwikkeling van nieuwe technologieën

Technische standaarden spelen een sleutelrol in de verdere ontwikkeling van het internet en nieuwe digitale technologieën. Standaarden bieden gedetailleerde specificaties over hoe een techniek moet werken, zodat deze voldoet aan bepaalde kwaliteitseisen en interoperabiliteit met andere producten mogelijk maakt, zelfs als deze van een andere fabrikant zijn. Dit geldt ook voor toepassingen die gebruikt kunnen worden voor controle of onderdrukking van burgers. De afgelopen jaren zien we dat de invloed van niet-westerse landen, waaronder bijvoorbeeld China, toeneemt op de ontwikkeling van standaarden voor nieuwe digitale technologieën zoals 5G, quantum, big data en AI. Dit heeft ook invloed op hoe het hierboven geschreven wegingskader wordt toegepast. De toegenomen aandacht voor digitale veiligheid en de vraag naar innovatieve oplossingen leidt ertoe dat ook in internationale standaardisatie organisaties steeds vaker gewerkt wordt aan standaarden die potentieel gevolgen kunnen hebben voor mensenrechten. Dit kan leiden tot nieuwe producten die op basis van technische standaarden, voor bijvoorbeeld quantum of kunstmatige intelligentie, mensenrechtenschendingen mogelijk maken.

Probleemstelling

Hoewel er genoeg staten zijn die nieuwe digitale technologie rechtmatig inzetten, is er ook een beweging naar de andere kant te zien. Door middel van onder andere nieuwe wetgeving, censuur, desinformatie, *shutdowns* en surveillance nemen online mensenrechtenschendingen toe. Daardoor wordt het internet in toenemende mate ingezet als instrument voor oppressie in plaats van als middel voor de bevordering van veiligheid, ontwikkeling en welvaart. Hoewel dit soort schendingen steeds vaker worden opgebracht in het multilaterale debat, verschuilen landen die zich hier schuldig aan maken zich vaak achter het argument dat over de toepassing van mensenrechten online nog geen internationale afspraken zijn gemaakt.

Daarnaast kunnen technologieën zoals gezichtsherkenning een waardevolle consumententoepassing hebben, maar ook ingezet worden om mensenrechten te schenden. Wanneer zulke standaarden vastgesteld worden in een multilaterale organisatie, valideert standaardisatie de toepassing van deze technieken en maakt het internationale handel in producten die deze technologie toepassen, makkelijker. Daarmee neemt de kans op mensenrechtenschendingen toe. Vanwege die ontwikkeling kan standaardisatie van nieuwe digitale technieken niet meer enkel vanuit technisch perspectief bekeken worden.

Antwoord

Strategische coalities voor erkenning en toepassing van internationaal recht en mensenrechten online

Voor het kabinet is het kraakhelder: internationaal recht en mensenrechten gelden zowel online als offline. Dit is ook erkend door de VN[9]. Principes die we hebben vastgelegd in internationale verdragen rondom goed bestuur, rechtstaat en mensenrechten moeten zoveel mogelijk direct vertaald worden naar de digitale omgeving. Soms is deze vertaling nog niet direct mogelijk, bijvoorbeeld omdat de technologie nieuw ontwikkeld is en de mensenrechtenrisico's daardoor nog niet zijn geïdentificeerd. In die gevallen werken we in een brede coalitie van landen, onderzoekers, bedrijven en maatschappelijk middenveld, aan een uitwerking hoe bestaande internationaal erkende principes zouden moeten worden toegepast.

Het kabinet zal in dat licht de komende jaren inzetten op uitbreiding van de *Freedom Online Coalitie* (FOC), die Nederland in 2011 heeft opgezet. Momenteel zijn 37 landen lid van deze coalitie. De FOC heeft zich gevormd tot een kopgroep die zich hard maakt voor de toepassing van online mensenrechten en spreekt zich middels gezamenlijke verklaringen uit over de toepassing van mensenrechten online op thema's waarover nog geen internationale consensus is bereikt. Goede voorbeelden hiervan zijn gezamenlijke verklaringen rondom het tegengaan van online desinformatie[10], of over mensen-

[9] Zie het aangenomen VN rapport (A-AC.290-2021-CRP.2) uit 2021 dat stelt: States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.
En de VN Mensenrechtenraad resolutie A/HRC/20/L.13 uit 2012: The promotion, protection and enjoyment of human rights on the Internet.

[10] Freedom Online Coalition, november 2022, Joint statement on Spread of Disinformation Online: https://freedomonlinecoalition.com/wp-content/uploads/2022/03/FOC-Joint-Statement-on-Spread-of-Disinformation-Online.pdf.

rechten en kunstmatige intelligente[11], digitale inclusie[12] en de 'leidende principes rondom overheidsinzet van surveillancetechnologie'[13]. Middels verklaringen en onderlinge coördinatie proberen de FOC-leden in VN-onderhandelingen te komen tot een zo sterk mogelijk resultaat.

De FOC is nu al een gevarieerde diplomatieke coalitie met landen uit alle continenten maar Nederland streeft naar verdere verbreding. Om de legitimiteit van de FOC te vergroten, en te illustreren dat deze onderwerpen een brede groep landen zorgen baart, is het zaak vooral meer opkomende landen aan te moedigen lid te worden van de coalitie. Naast diplomatieke coördinatie biedt de coalitie namelijk ook de mogelijkheden tot het delen van kennis en kunde over deze onderwerpen, om zo de capaciteit binnen overheden te vergroten. Om deze reden zet het kabinet erop in de FOC de komende 5 jaar met tenminste 10 leden te laten groeien, waarbij gemikt wordt op opkomende landen. Verder zal het kabinet het belang onderstrepen dat de Europese Unie en de *Freedom Online Coalition* toenadering tot elkaar zoeken.

Tegelijkertijd zal het kabinet zich ervoor inzetten dat andere diplomatieke coalities op dossiers die raken aan het cyberdomein nauw optrekken met de FOC. Hierbij richt het kabinet zich specifiek op de thema's democratie (*Internationale IDEA*), mediavrijheid (*Media Freedom Coalition*) en LHBTIQ+ rechten (*Equal Rights Coalition*).

Stimuleren van staten en bedrijven om online mensenrechtenschendingen tegen te gaan

Naast het uitdragen van de manier waarop internationaal recht en mensenrechten online van toepassing zijn, is het zaak om schendingen hiervan effectief te adresseren. Het kabinet zal de komende jaren een proactieve rol blijven pakken in het adresseren van online mensenrechtenschendingen of schendingen van andere internationale verdragen in de digitale omgeving. Dit kan middels bilateraal overleg, zowel publiekelijk als achter gesloten deuren, maar ook door middel van de hierboven genoemde coalities. De onlangs verschenen gezamenlijke verklaring van de *Freedom Online Coalition 'Internet Shutdowns in Iran'*[14] naar aanleiding van de vrouwenprotesten is hiervan een goed voorbeeld dat de komende jaren navolging moet krijgen.

De onrechtmatige inzet van technologieën door sommige staten voor digitale surveillance (zoals gezichtsherkenningstechnologie, big-data analyse of binnendringsoftware) is zorgelijk. Als Nederland zelf gebruik maakt van digitale technologieën voor opsporing of het beschermen van de nationale veiligheid gebeurt dat conform wet- en regelgeving en na een zorgvuldige afweging, waarbij principes van mensenrechten en rechtsstatelijkheid de kaders bepalen. Binnen de opsporing geldt als eis dat leveranciers van binnendringsoftware worden gescreend door de AIVD en dat zij geen producten mogen verkopen aan dubieuze regimes. Dit voorbeeld voor verantwoorde aanschaf zal het kabinet ook de komende jaren actief uitdragen. Dat de kaders van het internationale recht ook voor digitale middelen gelden, zal het kabinet blijven bepleiten.[15]
Op basis van deze kaders zal het kabinet diplomatieke middelen blijven inzetten om landen die deze technologieën misbruiken aan te spreken, waar mogelijk in EU-verband.

Bij de aanpak van online desinformatie en haatspraak is het van belang een balans te vinden tussen enerzijds het tegengaan van statelijke desinformatie en propaganda en anderzijds in te blijven zetten op een vrij en pluriform online medialandschap. De Nederlandse aanpak bestaat uit de volgende elementen: het beschermen en stimuleren van vrije media[16], het reguleren van tech-platforms en gerichte diplomatieke respons op desinformatie vanuit statelijke actoren. Deze combinatie beoogt dat overheden desinformatiecampagnes kunnen tegengaan zonder dat dit invloed heeft op de vrijheid van meningsuiting van individuele burgers. Hierin volgt het kabinet het advies van de AIV op dit onderwerp.[17] Daarnaast hebben Canada en Nederland tijdens de Algemene Vergadering van de VN te kennen gegeven samen te willen werken aan '*rules of the road*' voor het tegengaan van desinformatie. Het kabinet zal dit initiatief aangrijpen om met een internationale coalitie van landen te werken aan niet-bindende normen rondom informatie integriteit online, inclusief het tegengaan van online desinformatie, op een wijze die in overeenstemming is met mensenrechten en internationaal recht.

---

[11] Freedom Online Coalition, november 2022, Joint statement on Artificial Intelligence and Human Rights https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-Artificial-Intelligence-and-Human-Rights.pdf

[12] Freedom Online Coalition, februari 2022, Joint statement on Digital Inclusion https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-Digital-Inclusion.pdf

[13] Freedom Online Coalition, maart 2023, Guiding principles on government use of surveillance technologies https://freedomonlinecoalition.com/wp-content/uploads/2023/03/FOC_Guiding_Principles_on_Government_Use_of_Surveillance_Technologies.pdf

[14] Freedom Online Coalition, oktober 2022, Joint Statement on Internet Shutdowns in Iran: https://freedomonlinecoalition.com/wp-content/uploads/2022/10/FOC-Joint-Statement-on-Internet-Shutdowns-in-Iran_October-2022.pdf.

[15] Zo onderschreef het kabinet onlangs de gezamenlijke verklaring van de Freedom Online Coalitie omtrent verantwoorde inzet van surveillancetechnologie door overheden.

[16] EU Media Freedom Act

[17] AIV-advies 113: Regulering van online content: naar een herijking van het Nederlandse Internetbeleid d.d. 24 juni 2020; kabinetsreactie Kamerstuk 26643, nr. 858 d.d. 6 mei 2022

Naast staten hebben ook bedrijven een verantwoordelijkheid om mensenrechten online te respecteren. Vanwege hun kennis over de digitale producten die ze zelf ontwikkelen, zouden zij beter in staat moeten zijn om de risico's en effecten van hun product op het gebied van mensenrechten in kaart te brengen. De verantwoordelijkheid die bedrijven hebben, is onder andere neergelegd in de OESO Richtlijnen voor multinationale ondernemingen[18] en de *UN Guiding Principles on Business and Human Rights*[19]. Het kabinet zal zich ervoor inspannen dat deze richtlijnen beter door bedrijven worden nageleefd en zal ervoor pleiten dat deze vaker worden opgenomen in EU partnerschappen met derde landen. Ook zal het kabinet derde landen faciliteren in het contact met grote tech bedrijven en waar nodig schendingen in grotere coalities ter sprake brengen.

Steeds meer bedrijven hanteren encryptie, ook wel versleuteling, als onderdeel van hun online diensten. Hiermee wordt het recht op privacy, de vertrouwelijkheid en integriteit van communicatie en opgeslagen data beter beschermd waarmee encryptie helpt bij het weren van spionage en cybercriminaliteit. Hiertegenover staat dat encryptie de rechtmatige toegang tot gegevens voor opsporings- en inlichtingendiensten steeds moeilijker maakt. Dit maakt dat de toepassing van encryptie een veel besproken onderwerp is, zowel binnen de VN als de EU. Eerder is hierover het kabinetsstandpunt encryptie gepubliceerd[20], waarin wordt gesteld dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland en sterke encryptie te stimuleren. In de internationale context draagt het kabinet deze conclusie en de afwegingen die daaraan ten grondslag liggen uit.

Met regelgeving voor online platformen (*Digital Services Act* - DSA) of de verantwoorde inzet van kunstmatige intelligentie (AI-ACT) heeft de EU concrete, werkbare principes geformuleerd rondom toepassingen van AI en internetdiensten die mensenrechten en de rechtstaat respecteren. Hoe deze principes in de praktijk moeten worden toegepast, bijvoorbeeld in het toezichthouden op online contentmoderatie op basis van de DSA, is nog echter lang niet altijd even duidelijk. Dit geldt voor zowel de grote technologiebedrijven als de nationale toezichthouders. Om deze reden zal het kabinet een conferentie organiseren voor de verschillende toezichthouders uit de EU lidstaten over de toepassing van mensenrechten bij contentmoderatie. Tot slot draagt het kabinet de principes van de DSA en AI-act internationaal uit om zo het 'Brussel effect' te versterken. Hierbij is het doel niet alleen dat enkel de wet- of regelgeving door een zo groot mogelijke groep landen wordt omarmd. Zonder institutionele inbedding van democratie en rechtstaat kan wetgeving voor regulering van online platformen gebruikt worden voor bijvoorbeeld censuur. Het kabinet zal daarom bij landen die deze EU wetgeving (gedeeltelijk) overnemen ook nadrukkelijk pleiten voor implementatie van mensenrechtelijke en democratisch principes.

Waarborging van mensenrechten en democratische beginselen bij ontwikkeling en standaardisatie van nieuwe technologieën

De ontwikkeling van nieuwe technologie kan niet los worden gezien van internationale afspraken over mensenrechten en democratie. Het in kaart brengen van de mensenrechtenrisico's in de toepassing van dit soort nieuwe technologieën moet daarom een vast onderdeel worden van de ontwikkeling van nieuwe technologische producten.
De Staatssecretaris van Digitale Zaken heeft hier de afgelopen tijd al stappen op ondernomen om dit binnen Nederland vorm te geven.[21] Het kabinet zal erop inzetten om de komende jaren dit beleid ook buiten Nederland en de EU onder de aandacht te brengen, zodat deze *Human Rights Impact Assessments* een vast en betrouwbaar onderdeel worden in de ontwikkeling van nieuwe technologische producten. Hiermee bouwt deze Internationale Cyberstrategie voort op de Werkagenda Waardengedreven Digitaliseren.[22]

Aangezien standaarden een belangrijke rol spelen in het op de markt brengen van opkomende technologieën, moet in het standaardiseringsproces rekening gehouden worden met mogelijke risico's voor mensenrechten. Het kabinet zal de ontwikkelingen van nieuwe technische standaarden nauwlettend in de gaten houden. Hierbij heeft het kabinet vooral aandacht voor de toenemende politisering van de van oorsprong technische standaardisatieorganisaties.
Ook zal aandacht worden gevraagd voor de toepasbaarheid van de UN *Guiding Principles on Business and Human Rights* in standaardisatieprocessen.

Het is aannemelijk dat de ontwikkeling van nieuwe technologieën, zoals AI en quantumtechnologie, naast een breed palet aan nieuwe mogelijkheden ook zal leiden tot nieuwe risico's voor mensenrechten en democratie. Nu AI meer concrete toepassingen krijgt, neemt ook het kennisniveau over deze risico's toe, maar rondom quantum blijft dit nog uit. Het kabinet zal in dat licht een onderzoek laten doen naar de mensenrechtenrisico's van nieuwe digitale technologieën en hierover in overleg treden met de cybersecurityraad.

[18] Zie voor een Nederlandse vertaling: https://www.oesorichtlijnen.nl/oeso-richtlijnen
[19] 2011, Guiding Principles on Business and Human Rights, Bureau van de Hoge Commissaris van de Verenigde Naties voor de Mensenrechten, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
[20] Zie kamerbrief 26643-383
[21] Zie kamerbrief 32761-262
[22] Zie kamerbrief 26643-940

Strategische doelstelling 3

Behoud van een wereldwijd open, vrij en veilig internet

Resultaatgebieden
- Bescherming van de publieke kern van het internet
- Grotere betrokkenheid van opkomende landen bij het beheer en doorontwikkeling van de publieke kern van het internet
- Vergroten cybercapaciteiten in opkomende landen

Analyse

De Nederlandse economie en samenleving kunnen niet functioneren zonder een stabiele en veilige digitale infrastructuur. Het internet als wereldwijd verbonden netwerk van netwerken vormt het fundament onder onze digitale wereld. De publieke kern van het internet zorgt dat deze wereldwijde verbondenheid gerealiseerd en gegarandeerd wordt. Deze kern wordt vormgegeven door een brede schakering van instituties, protocollen en standaarden op basis van gedeelde normen, waarden en doelen. Deze kern vormt het fundament dat de duurzame ontwikkeling van nieuwe en innovatieve toepassingen mogelijk maakt, die op hun beurt weer bijdragen aan wereldwijde groei en welvaart.

Multistakeholder-organisatie van het internet

Het brede toepassingsgebied en de verscheidenheid aan toepassingen en gebruikers maakt het beheer en de ontwikkeling van deze technische kern complex. Het proces van *internet governance* is gebaseerd op het multistakeholder-model[23], waarbij alle belanghebbenden op gelijke voet kunnen meekijken, praten en beslissen over ontwikkelingen van en wijzigingen in de publieke kern van het internet. Het multistakeholder-model is voornamelijk van toepassing wanneer het gaat over afspraken over het internet zelf, het beheer en uitgifte van IP-adressen en de technische standaarden die communicatie en interoperabiliteit tussen de netwerken en applicaties faciliteren. Deze open samenwerking tussen de belanghebbenden is belichaamd in organisaties zoals de *Internet Corporation for Assigned Names and Numbers* (ICANN), *Internet Engineering Task Force* (IETF), *World Wide Web Consortium* (W3C) en het *Institute of Electrical and Electronics Engineers* (IEEE). Deze organisaties spelen een faciliterende rol bij aanpassingen van technologieën, standaarden en procedures die de publieke kern van het internet vormgeven.

De komende jaren zullen cruciaal zijn voor behoud van dit model. Tijdens de *World Summit on Information Society* (WSIS) in 2005 zijn afspraken gemaakt die aan de basis liggen van het multistakeholdermodel van het internet governance[24]. De komende jaren worden deze afspraken geëvalueerd, wat mogelijk in aanloop naar de WSIS+20 in 2025 leidt tot een heronderhandeling over de manier waarop *internet governance* momenteel is vormgegeven.

Geopolitieke strijd om het beheer van het internet

De neutrale, apolitieke en technische benadering van de publieke kern staat al langer onder druk.[25] Staten als Rusland en China bepleiten een verschuiving van het beheer van het internet naar multilaterale organisaties, zoals bijvoorbeeld de *International Telecommunications Union* (ITU), de VN-organisatie voor informatie- en communicatietechnologie en proberen daar zoveel mogelijk steun voor te vergaren. Interstatelijke samenwerking is in de ITU de norm, en de belangen van niet-statelijke stakeholders,

[23] De ontwikkeling en toepassing door overheden, de technische gemeenschap, de private sector, het maatschappelijk middenveld en academici van gedeelde principes, normen, besluitvormingsprocedures en programma's die de ontwikkeling en het gebruik van het Internet als wereldwijd verbonden netwerk vormgeven.

[24] Zie WSIS Outcome documents - December 2005 (itu.int). Onderdeel van de afspraken is de Tunis Agenda, waarin internet governance wordt gedefinieerd als een multistakeholder proces. Ook is dit document de basis voor organisatie van het Internet Governance Forum – het VN platform waar overheden, bedrijven, academici en internet organisaties elkaar jaarlijks over internet governance spreken.

[25] Vanaf het moment dat de mondiale impact van Internet duidelijk werd (in de loop van de jaren negentig), is discussie geweest over de gewenste internationale structuren voor Internet governance. Voor een historische schets van deze discussie, zie bijv. het AIV-advies no. 92 (november 2014), pp 16 e.v.

zoals bedrijven, maatschappelijke organisaties en de technische gemeenschap, worden er minder gehoord.

Tegelijkertijd worden ook binnen de EU regelmatig voorstellen gedaan voor wetgeving die, in een poging de interne markt te versterken, onbedoeld het multistakeholder model dreigen te ondermijnen. Zo zijn er diverse richtlijnen die elementen van het domeinnaamsysteem (DNS) reguleren, iets wat traditioneel via het multistakeholder proces wordt vormgegeven. Deze wetgeving inspireert en valideert mogelijk andere landen om hetzelfde te doen, wat het multistakeholder proces aan belang doet inboeten.

Tot slot zien we dat politieke en economische sancties (waaronder de beperkende maatregelen die de EU kan opleggen) organisaties kunnen raken die een rol spelen bij het in standhouden van de publieke kern van het internet. Op die manier kunnen sancties onbedoeld leiden tot versnippering van, of schade aan, de mondiale technische infrastructuur van het internet of aan het internationale systeem voor *internet governance*. Voorbeelden hiervan zijn de *Regional Internet Registries*, onafhankelijke organisaties die de toewijzing en registratie van onder andere IP-adressen overzien.

Internetfragmentatie

Wanneer wordt ingegrepen in de organisatie, beheer en administratie van het internet dreigt de wereldwijde interoperabiliteit verloren te gaan. Wanneer een land of groep landen de autoriteit van de multistakeholder organisaties of het belang van het multistakeholder model niet meer erkent, kan dit leiden tot een fragmentatie van de publieke kern. Dit zou betekenen dat er verschillende internetsystemen (een vrij en een staatsgestuurd internet) naast elkaar bestaan. Een dergelijke splitsing zal de communicatie tussen landen, zoals e-mail en bellen via het internet en daarmee ook het handelsverkeer aanzienlijk verstoren, met potentieel grote en zeer schadelijke gevolgen voor wereldwijde economische ontwikkeling en de geopolitieke stabiliteit.

Connectiviteit en cyberveiligheid in opkomende landen

Belangrijk onderdeel van de discussie over het beheer van het internet is dat een groot deel van de wereld hier nog niet actief bij betrokken is. Een aanzienlijk aantal landen kampt met beperkte of gebrekkige connectiviteit, dat vaak samengaat met een gebrekkige digitale veiligheids-infrastructuur. Hoewel het overbruggen van de digitale kloof al breed wordt geadresseerd, door bijvoorbeeld Nederland, de EU en Wereldbank, worden de noodzaak van cyberweerbaarheid en verantwoord bestuur niet altijd meegenomen in digitaliseringsprocessen. Dit maakt dat in het merendeel van de landen wereldwijd de digitale infrastructuur, de ICT-systemen en gebruikte software onveilig zijn, met alle gevolgen voor de data- en netwerkveiligheid en de veiligheid van de eindgebruikers. Dat heeft gevolgen op lokaal maar ook op internationaal niveau aangezien een netwerk zo sterk is als haar zwakste schakel waardoor lokale veiligheidslekken geëxploiteerd kunnen worden voor aanvallen in andere landen.

Probleemstelling

De manier waarop het internet tot nu toe is vormgegeven en wordt beheerd, zal de komende jaren worden geëvalueerd. Grote wijzigingen in het *governance*-model kunnen leiden tot fragmentatie van het internet met potentieel grote geopolitieke en sociaaleconomische gevolgen.
Om het internet open, vrij en veilig te houden, is het van groot belang de betrokkenheid van niet-statelijke stakeholders zoals private sector, academici, maatschappelijke organisaties en de technische gemeenschap bij de discussie over het beheer van het internet te vergroten. Ook zijn veel opkomende landen nog niet actief genoeg bij deze discussies betrokken. Dat lijkt te worden veroorzaakt doordat veel van deze landen de handen vol hebben aan meer operationele uitdagingen op het gebied van digitalisering en cyberveiligheid waardoor zij zich (nog) niet actief bemoeien met de internationale discussies over het beheer van het internet.

Antwoord

Bescherming van de publieke kern van het internet

Behoud van de eenheid van de publieke kern van het internet staat wat het kabinet betreft centraal om fragmentatie te voorkomen. De publieke kern moet – zo concludeerde de WRR al in een rapport uit 2015 – gevrijwaard blijven van oneigenlijk interventies van staten en andere partijen die schade toebrengen en het vertrouwen in het internet eroderen.[26] Deze eenheid kan het beste behouden worden middels bescherming en versterking van het multistakeholder-model voor beheer van het internet.

De bescherming van de publieke kern staat daarom sinds 2015 hoog op de Nederlandse agenda.

Het beheer van het internet is belegd bij het ministerie van EZK, dat Nederland vertegenwoordigt in ICANN en het *Internet Governance Forum*. Het kabinet blijft erop inzetten om via organisaties en partnerschappen[27] connectiviteit voor alle landen te vergroten, wet- en regelgeving en het beheer te verbeteren en politisering van de publieke kern tegen te gaan om fragmentatie van het internet te voorkomen.

[26] De publieke kern van het internet. Naar een buitenlands internetbeleid | Rapport | WRR
[27] Zoals de EU Global Gateway, ITU-Development en Digital4Development hub.

Zo pleiten we binnen de VN voor erkenning van het niet-politieke karakter van deze "publieke kern" en zetten we ons bij *internet governance* fora in voor de versteviging en de onafhankelijkheid ervan.

Het kabinet zal de komende jaren in multilaterale onderhandelingen (zoals bijvoorbeeld de *Global Digital Compact* en de *WSIS+20 review* van de Verenigde Naties) een leidende rol nemen om zowel de publieke/technische kern van het internet als de noodzakelijke toepassing van het multistakeholder model in nieuwe multilaterale afspraken vast te leggen.

Naast bescherming van het multistakeholder-model zal het kabinet ook de risico's van internet fragmentatie laten onderzoeken. Hierbij moet gekeken worden naar zowel de politieke en technische afhankelijkheden, alsmede de economische gevolgen van fragmentatie. Doel van het onderzoek is om hiermee niet alleen de risico's voor Nederland in kaart te brengen, maar ook inzichtelijk te maken voor derde landen (binnen en buiten de EU) wat de mogelijke gevolgen hiervan zijn en deze bij het Internet Governance Forum en andere multilaterale fora onder de aandacht te brengen.

Tot slot zal het kabinet er voor pleiten dat organisaties die een belangrijke rol spelen bij het functioneren van de publieke kern van het internet niet geraakt moeten kunnen worden door beperkende maatregelen als sancties.
Dat gesprek zal het kabinet allereerst binnen de EU en later ook binnen andere coalities aanjagen. Indien organisaties zoals *Regional Internet Registries* worden geraakt door EU- of andersoortige sancties, speelt dat landen in de kaart die bepleiten dat het Westen met sancties de discussie over de werking van het internet politiseert.

Grotere betrokkenheid van opkomende landen bij het beheer van het internet

Met het groeiende belang van het internet en digitalisering in opkomende landen profileren zij zich ook sterker in de discussie over het beheer van de publieke kern. Hoewel opkomende landen niet altijd onze posities rondom mensenrechten online delen, worden de algemene principes rondom het technisch beheer van het internet en de toepassing van internationaal recht online over het algemeen wel erkend[28]. Zo ondertekende een groot aantal opkomende landen de *Declaration for the Future of the Internet*[29], waarin het belang van de hierboven beschreven principes onderstreept werd. Omdat het relatieve belang van opkomende landen op het internationale podium toeneemt, wil het kabinet de samenwerking stimuleren, versterken en verbreden. Met betrokkenheid van een grotere groep landen wordt de internationalisering verder vergroot en de legitimiteit van het huidige *internet governance* model versterkt.

Hierbij richt het kabinet zich in het bijzonder op de Westelijke Balkan, Azië en Oceanië en landen in zuidelijk Afrika. Door middel van regionale cyberdialogen waar voor de regio relevante cyberonderwerpen worden besproken, cursussen om cyberweerbaarheid te vergroten en samenwerking in fora zoals de Verenigde Naties wil het kabinet ervaringen uitwisselen en de relatie met nieuwe partners verstevigen. We gaan het gesprek aan over hoe we gezamenlijk algemene principes rondom het technisch beheer van het internet en de toepassing van het internationale recht online het beste kunnen verstevigen.

Vergroten cybercapaciteiten in opkomende landen

Het enkel intensiveren van de diplomatieke inzet om betrokkenheid te vergroten van opkomende landen bij *internet governance* processen is niet voldoende. In het eerder aangehaalde rapport maakt de WRR bij de definiëring van de veiligheid van het internet onderscheid tussen de benadering van 'nationale veiligheid' (waarin nationale belangen boven de belangen van het netwerk gaan) en 'technologische veiligheid' (waarin de veiligheid van het netwerk als geheel centraal staat). Om de neutraliteit en effectieve werking van de publieke kern te kunnen blijven garanderen, moet die tweede benadering worden nagestreefd.

Daarin zijn de *Computer Security Incident Response Teams* (CSIRT's), die veel landen in het leven hebben geroepen, belangrijke partners. Om die reden zal het kabinet haar inzet versterken om opkomende landen te assisteren hun 'CSIRT's op te zetten of verder te ontwikkelen. Zo functioneren CSIRT's vaak onder de maat als gevolg van nog gebrekkige kennis, capaciteit en regelgeving. Het Nationaal Cyber securitycentrum (NCSC) is gestart met de uitvoering van een project voor capaciteitsopbouw dat onder andere ziet op het ontwikkelen en uitvoeren van trainingen. Het NCSC is voor de Nederlandse overheid de verbindende schakel in een netwerk van nationale en internationale partners.
Tijdens ernstige cyberincidenten met mogelijke effecten buiten Nederland, fungeert het NCSC als eerste nationale contactpunt voor EU-lidstaten.

Via samenwerking met partners als het *Global Forum on Cyber Expertise* (GFCE), een wereldwijd netwerk van 180 landen,

[28] Zoals bijvoorbeeld de organisatie van het internet middels het multistakeholder model en het feit dat de organisaties die het beheer en administratie van het internet aan de hand van deze consensus uitvoeren.

[29] *Declaration for the Future of the Internet*, Een verklaring die op 28 april 2022 door de EU, VS, en de andere landen uitgebracht is. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_2695/IP_22_2695_EN.pdf

organisaties en bedrijven, wordt aandacht besteed aan het versterken van cyberweerbaarheid en -expertise van derde landen. Dit in 2015 door Nederland gelanceerde platform organiseert werkgroepen rond cyberveiligheid, cybercriminaliteit en de bescherming van kritieke infrastructuur. Daarnaast tracht het GFCE de wensen en behoeften in opkomende landen in kaart te brengen en hier de juiste uitvoerder bij te vinden.

Digitalisering bespaart kosten, creëert economische kansen en versterkt het investeringsklimaat in zowel lage, midden als hoge inkomenslanden. Het zorgt voor betere verbindingen tussen mensen en biedt zo kansen om de SDG's versneld te bereiken. Het meenemen van cyberweerbaarheid in project design is daarom van groot belang maar de uitvoering ervan blijkt vaak uitdagend. De Nederlandse inzet op digitalisering wordt in de strategie voor Buitenlandse Handel en Ontwikkelingssamenwerking (BHOS) 'Doen waar Nederland goed in is' uitvoerig beschreven. In de komende jaren weegt het kabinet binnen de bestaande strategie en middelen ook cyberweerbaarheid nadrukkelijk mee in de digitaliseringsprojecten uit de BHOS-strategie en vraagt hier – samen met gelijkgezinde landen - eveneens aandacht voor bij de uitvoering van soortgelijke EU en VN-projecten.

In Europees verband zoekt het kabinet aansluiting bij de *Global Gateway*[30]-strategie van de Europese Commissie en de Hoge Vertegenwoordiger; het nieuwe kader om de connectiviteit tussen de EU en de rest van de wereld, onder andere op het gebied van digitalisering, te versterken door middel van grootschalige investeringen. *Digital Economy Packages* combineren investeringen in digitale infrastructuur met land-specifieke bijstand om regelgevingskaders te ontwikkelen op basis van cyberveiligheid en privacy. Ook zoeken we aansluiting bij de agenda van de *UN Tech Envoy*, gericht op digitale inclusiviteit en duurzame toegang tot nieuwe technologieën. Dit zal zijn beslag krijgen in de *Global Digital Compact* die naar verwachting tijdens de *Summit of the Future* in september 2024 wordt aangenomen.

Het kabinet zal een vraag gestuurde benadering hanteren en zo nodig nationale expertise inzetten om bijvoorbeeld wetgeving in lijn te brengen met het Budapest verdrag (cybercriminaliteit), beleid te formuleren om kritieke infrastructuur te beschermen of te assisteren bij de vertaling van internationaal recht naar de rechtstaat online. Het netwerk van cyberdiplomaten op de 34 ambassades en Permanente Vertegenwoordigingen speelt een cruciale rol in het verbinden van onderhouden van deze nieuwe en bestaande partnerschappen en initiatieven.

[30] Deze nieuwe EU-strategie stimuleert veilige verbindingen wereldwijd. Hiertoe heeft de EU een ambitieus infrastructureel plan ontwikkeld dat tussen 2021 – 2027 door de EU-instellingen en de EU-lidstaten zal worden uitgevoerd.

Bijlage activiteitenoverzicht

Doelstelling	Resultaatgebied	Activiteit	Coördinerende departementen/organisaties
Tegengaan van cyberdreigingen van staten en criminelen	Van reactieve naar proactieve omgang met cyberdreigingen	• De proactieve benadering wordt uitgewerkt in een strategisch kader. • Daarbinnen worden mogelijkheden voor samenwerking met de private sector bij het adresseren van cyberdreigingen in kaart gebracht.	BZ, NCTV, J&V, DEF, NCSC, AIVD, MIVD, OM, Politie
	Vergroten van het zicht op de dreiging	• Er wordt geïnvesteerd in de onderzoekscapaciteit van de Inlichtingen- en Veiligheidsdiensten ten behoeve van inlichtingenmatig diepteonderzoek. • Informatie over (hybride) dreigingen wordt frequenter met partners en met relevante partijen in de Nederlandse samenleving gedeeld. • Met de Tijdelijke Wet Cyberoperaties beoogt het kabinet de diensten, met behoud van waarborgen, in staat te stellen hun bevoegdheden sneller en effectiever in te kunnen zetten in het digitale domein.	AIVD, MIVD AIVD, MIVD AIVD, MIVD
	Versterkte slagkracht in het cyberdomein	• Cyber expertise wordt aangetrokken om de offensieve en defensieve cybercapaciteiten uit te breiden. • Er wordt geïnvesteerd in de integratie van cybermiddelen bij en tussen alle operationele commando's. Tevens worden de cyber- en elektromagnetische capaciteiten van de defensieonderdelen versterkt.	DEF DEF

Doelstelling	Resultaatgebied	Activiteit	Coördinerende departementen/organisaties
	Slagvaardige internationale coalities	• Nederland neemt het voortouw bij de versterking van de EU cyberdiplomacy toolbox, in het bijzonder ten aanzien van het cybersanctieinstrumentarium.	BZ
		• Binnen de EU wordt ingezet op het vergroten van de synergie tussen de cyberdiplomacy toolbox en aanverwante instrumenten zoals de *hybrid toolbox* en de toolbox voor Foreign Information Manipulation and Interference.	BZ
		• Ervaringen uit de EU bij het tegengaan van kwaadwillende cyberoperaties worden gebruikt om de samenwerking binnen de NAVO te versterken, vooral via door-ontwikkeling van de NAVO-guide.	BZ, DEF
		• Informatieuitwisseling over cyberdreigingen en multilaterale processen wordt met partners buiten de EU en NAVO wordt uitgebreid, onder andere met Japan, Zuid-Korea, Singapore, Australië en Nieuw-Zeeland.	BZ
		• Bilaterale cyberbetrekkingen worden geïntensiveerd, onder andere door het opzetten van meer 'cyberdialogen' met derde landen. Aandacht daarbij gaat primair uit naar landen in Afrika en de Indo-Pacific.	BZ
		• Inzet van 'regionale cyberdialogen' (waarbij landen uit een regio met elkaar in gesprek gaan over o.a. cyberwetgeving, internationaal recht en multilaterale processen) wordt gecontinueerd. Aandachtsregio's zijn de Westelijke Balkan, Zuidelijk Afrika en Zuidoost-Azië.	BZ
		• Gesprekken met derde landen over het vergroten van de cyberveiligheid van kritieke infrastructuur (waaronder in de maritieme sector) worden geïntensiveerd.	NCTV, I&W, EZK, NCSC
	Versterking en bestendiging van normen voor verantwoord statelijk gedrag	• Nederland neemt het initiatief voor verdere internationale afspraken gericht op de risico's van nieuwe technologieën zoals AI en kwantum voor internationale cyberveiligheid.	BZ, EZK, J&V
		• I.s.m. partners neemt NL voortouw om de implementatie en naleving van het normatief kader voor verantwoord statelijk gedrag in het cyberdomein te bevorderen via de uitwerking van de *Programme of Action* waarover de AVVN resolutie 77/73 aannam.	BZ
		• Via intensivering van bilaterale cyberbetrekkingen poogt Nederland landen te helpen het normatief kader te implementeren.	BZ
		• De Nederlandse bijdrage wordt vergroot aan het *Women in Cyber*-programma waarmee de deelname van vrouwelijke vertegenwoordigers aan multilaterale cyberprocessen wordt versterkt.	BZ
		• Nederland neemt het voorzitterschap van de Informal Working Group van de OVSE op zich. Nederland zal daarbij de aandacht leggen op bestendiging en uitvoering van de Confidence Building Measures.	BZ, NCSC

Doelstelling	Resultaatgebied	Activiteit	Coördinerende departementen/organisaties
	Versterkte internationale samenwerking tegen cybercriminaliteit	• Er wordt actief bijgedragen aan het door de VS geïnitieerde counter-ransomware initiatief. • Nederland zet zich ervoor in dat de komende jaren ten minste 10 Afrikaanse, Aziatische en/of Latijns Amerikaanse landen de Boedapest-conventie omarmen. • In de onderhandelingen over het cybercrime verdrag van de VN streeft NL naar een verdrag dat de aanpak van cybercrime effectief versterkt en waarbij effectieve voorwaarden en waarborgen (waaronder online vrijheden) zijn opgenomen;	J&V, BZ J&V, BZ J&V, BZ
Versterken van democratische en mensenrechtelijke principes online	Strategische coalities voor erkenning en toepassing van internationaal recht en mensenrechten online	• Nederland zet zich in voor uitbereiding (vooral met niet-westerse landen) van de Freedom Online Coalitie met ten minste vijf landen uit onze focusgebieden. • De synergie tussen de FOC en Internationale IDEA, de Media Freedom Coalition en de Equal Rights Coalition) wordt vergroot. • Nederland stelt zich kandidaat voor het voorzitterschap van de Freedom Online Coalition in 2024.	BZ BZ BZ

Doelstelling	Resultaatgebied	Activiteit	Coördinerende departementen/organisaties
	Stimuleren van staten en bedrijven om online mensenrechtenschendingen tegen te gaan	• Nederland moedigt i.s.m. Europese partners derde landen aan EU-eisen aan de export van binnendringsoftware over te nemen.	BZ, J&V, EZK
		• Nederland neemt het voortouw in het opzetten van een internationaal coalitie rondom contentmoderatie, onder andere om desinformatie en hate speech tegen te gaan.	BZ, J&V
		• Samen met Canada ontwikkelt Nederland zgn. “rules of the road” voor het tegengaan van desinformatie.	BZ, J&V
		• Het kabinet brengt in kaart hoe bedrijven gestimuleerd kunnen worden Human Rights Impact Assessments mee te wegen bij de toepassing van nieuwe technologische producten en tracht met bedrijven een code of conduct overeen te komen.	BZ, EZK, J&V
		• Er wordt een conferentie georganiseerd voor de verschillende toezichthouders uit de EU lidstaten over de toepassing van mensenrechten bij contentmoderatie in de toepassing van de DSA.	BZ, J&V, BZK, EZK
		• Binnen de werkagenda digitalisering is toezicht geborgd op een goede uitvoering van de DSA. Nederland ondersteunt doelen van de CoP, onder meer door samen te werken met partijen buiten de overheid.	BZK
		• BZK ziet erop toe dat door wetenschappers een pilot over verantwoorde datadeling wordt opgezet om inzicht te krijgen in onder andere de bescherming van kinderrechten online. Daarnaast krijgen onderzoekers meer structureel toegang tot online platforms zoals mogelijk gemaakt binnen de DSA.	BZK
		• Via de werkagenda digitalisering worden publieke media en instellingen ondersteund bij het ontwikkelen van een eigen infrastructuur en sociale mediaomgevingen die voldoen aan publieke waarden, zodat er een pluriformer digitaal medialandschap ontstaat.	BZK
		• Er wordt capaciteit gecreëerd binnen het Nederlands consulaat in San Francisco t.b.v. dialoog met tech bedrijven, coordinatie met partnerlanden en het vertalen van de stem van zuidelijke landen richting big tech.	BZ
	Waarborging van mensenrechten en democratische beginselen bij standaarden voor nieuwe technologieën	• In contacten met derde landen worden de principes en waarden van de Europese regelgeving ten aanzien van contentregulering en de verantwoorde inzet van AI actief uitgedragen. Europese partners worden aangespoord hetzelfde te doen.	BZ
		• Er wordt onderzoek gedaan naar de mensenrechtenrisico’s van nieuwe digitale technologieën en treedt hierover in overleg met de cybersecurityraad.	BZ, NCTV, J&V, EZK

Doelstelling	Resultaatgebied	Activiteit	Coördinerende departementen/organisaties
Behoud van een wereldwijd open, vrij en veilig internet	Bescherming van de publieke kern van het internet	• Nederland draagt zorg voor waarborging van het belang van de publieke/technische kern van het internet in de multiltarale processen *WSIS+20*, de *Global Digital Compact* en de *Summit of the Future* van de VN. • In samenwerking met gelijkgezinde landen zorgt Nederland ervoor dat niet-statelijke actoren (maatschappelijke organisaties, bedrijven, academici) een betekenisvolle bijdrage kunnen leveren aan deze trajecten. • Er wordt onderzoek gedaan naar de politieke, economische en bredere maatschappelijke risico's van internet fragmentatie. • Binnen de EU, maar ook richting gelijkgezinde landen, wordt gepleit voor de brede erkenning dat organisaties die van belang zijn voor het neutraal functioneren van de publieke kern van het internet niet geraakt mogen worden door beperkende maatregelen als sancties.	EZK, BZ BZ, EZK EZK, BZ BZ
	Grotere betrokkenheid van opkomende landen bij het beheer van het internet	• Via intensivering van de contacten met opkomende landen (onder meer via bilaterale en regionale dialogen) wordt de betrokkenheid van die landen bij discussies over het beheer van het internet versterkt.	BZ, BHOS
	Vergroten cybercapaciteiten in opkomende landen	• Er wordt een *Checklist Privacy & Security in Development Programmes* opgesteld om cyberweerbaarheid onderdeel te laten zijn van relevante digitaliseringsprojecten uit de BHOS-notitie. • De inzet om landen bij te staan om hun CERT verder te ontwikkelen, wordt geïntensiveerd. • Landen worden aangemoedigd om het EU-adequaatheidsbeginsel te implementeren. Hiermee kunnen via EU-conforme wettelijke waarborgen (bescherming persoonsgegevens) data worden uitgewisseld.	BHOS NCSC NCSC

Deze brochure is een uitgave van:

Het ministerie van Buitenlandse Zaken

Postbus 20061 | 2500 EB Den Haag