VERSLAG VAN EEN SCHRIFTELIJK OVERLEG
Vastgesteld, .. 2023

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 zijn brief van 9 juni 2023 over de Internationale Cyberstrategie (ICS) 2023-2028, (Kamerstuk 26643, nr. 1036).

De op 6 september 2023 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,
Heerema

De griffier van de commissie,
Westerhoff

Inhoudsopgave

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met interesse kennisgenomen van de inhoud van de Internationale Cyberstrategie 2023-2028. Hierover hebben zij nog enkele vragen en opmerkingen.

De leden van de VVD-fractie hebben een vraag over de constatering bij ‘doelstelling 1’ dat ook cyber-operaties onder de drempel van een gewapend conflict cumulatief het effect kunnen benaderen van de effecten die met een gewapend conflict worden bereikt. Is het kabinet van mening dat de cumulatieve effecten ook significant kunnen zijn als zij een strategisch effect hebben op de geopolitieke machtsverhoudingen, zoals bijvoorbeeld de Noord-Koreaanse

campagne om valuta te stelen en zo weerstand te bieden aan VN-sancties tegen haar nucleaire programma? Indien het kabinet deze analyse onderschrijft, is zij van mening dat hiertegen ook, idealiter via coalities van gelijkgezinde landen, opgetreden dient te worden? Ten aanzien van de ambitie proactief op te treden tegen cyberdreigingen vragen de leden van de VVD-fractie of het kabinet het eens is met het standpunt van onder meer Estland dat collectieve tegenmaatregelen in de cybercontext volkenrechtelijk gerechtvaardigd kunnen zijn? Zo nee, waarom niet? Zo ja, hoe is het kabinet van plan dit standpunt uit te dragen en samen met bondgenoten handelingsperspectief te creëren? Hierbij vragen de leden van de VVD-fractie ook of het kabinet van mening is dat de cumulatieve effecten van meerdere cyberaanvallen, eventueel begaan tegen meerdere landen in bijvoorbeeld de Europese Unie (EU) of de NAVO, bij elkaar opgeteld kunnen worden om te komen tot één internationale onrechtmatige daad, waarop een collectieve tegenmaatregel genomen kan worden? Vanaf welke vorm zou dit ook onder een "gewapende aanval" vallen, als bedoeld in artikel 5 van het Noord-Atlantisch Verdrag?

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

De leden van de VVD-fractie lezen dat het kabinet inzet op versterking en verduidelijking van de toepassing van het bestaande internationale recht in het cyberdomein. Zij merken op dat het kabinet hier wel een proces beschrijft, maar niet aangeeft hoe het deze normen dan precies ziet. Kan het kabinet hier meer duidelijkheid over geven? Wanneer is er bijvoorbeeld sprake van een onrechtmatige daad als, ook zonder het gebruik van fysiek geweld, het *domaine réservé* van een staat geschonden wordt door bijvoorbeeld inmenging in nationale verkiezingen? En ziet het kabinet bijvoorbeeld de Russische cyberaanvallen op Georgië van 28 oktober 2019 als een onrechtmatige daad? De leden van de VVD-fractie vragen in deze context ook of het kabinet de analyse deelt dat het duidelijk uitspreken als er sprake is van een onrechtmatige daad, kan bijdragen aan de vorming van internationaal gewoonterecht? Zo nee, waarom niet? Zo ja, is het kabinet bereid in de toekomst dergelijke uitspraken te doen, bij voorkeur samen met gelijkgezinde landen? En is het kabinet van mening dat het uitdragen van een dergelijke *opinio juris* effectiever kan zijn om langs het gewoonterecht tot normen te komen dan de vruchteloze pogingen om samen met landen als China en Rusland tot een verdrag te komen?

Vragen en opmerkingen van de leden van de D66-fractie

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

Tevens zijn de leden van de D66-fractie van mening dat de oorlog ook de noodzaak tot het tegengaan van toenemende desinformatie met betrekking tot de NAVO heeft blootgesteld. Deze leden vinden het daarom belangrijk dat het kabinet zich extra inzet om toenemende desinformatie rondom de NAVO tegen te gaan (bijvoorbeeld in de “Global South” en landen rondom Rusland) en hierbij nauwere samenwerking te zoeken met andere bondgenoten binnen de alliantie. De leden van de D66-fractie vragen wat de strategie is voor de privaat-publieke samenwerking om de verspreiding van desinformatie en propaganda tegen te gaan. Welke rol hebben tech-bedrijven volgens de minister en hoe draagt deze cyberstrategie eraan bij om daartoe te komen? De leden van de D66-fractie constateren dat de laatste jaren de invloed van autoritaire regimes op het vrije internet alleen maar is toegenomen, waardoor samenlevingen in verschillende delen van de wereld te maken krijgen met toenemende censuur als het gaat om vrijheid van meningsuiting en persvrijheid, maar ook desinformatie. Deze leden vragen wat de strategie van het kabinet is om deze mondiale risico’s voor het vrije internet, in samenwerking met onze bondgenoten, het hoofd te bieden. De leden van de D66-fractie zijn voorts benieuwd in hoeverre de uitwisseling van informatie tussen de bondgenoten binnen de EU en de NAVO inzake agressieve cyberstrategie van diverse (non-)statelijke actoren, veilig en beschermd is en niet in handen zal vallen van deze (non-)statelijke actoren.

Vragen en opmerkingen van de leden van de CDA-fractie

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van de Internationale Cyberstrategie 2023-2028. Deze leden hebben nog enkele vragen en opmerkingen. Zij lezen dat diverse technologische ontwikkelingen, zoals gezichtsherkenningstechnologie en big-data analyse en software, worden misbruikt voor politieke controle. De ontwikkeling van nieuwe technologieën, zoals AI en quantumtechnologie, zullen ook leiden tot nieuwe risico’s voor mensenrechten en democratie. Deze leden lezen echter in de strategie niks over mogelijke exportrestricties op dergelijke nieuwe technologieën die kunnen worden ingezet voor mensenrechtenschendingen. In het recente verleden bleek dat Europese en Nederlandse bedrijven surveillancetechnologieën leveren aan China[1]. Zijn exportrestricties een beleidsoptie, vragen deze leden. De leden van de CDA-fractie zijn ook benieuwd naar de stand van zaken omtrent samenwerking op het gebied van de ontwikkeling van nieuwe technologieën tussen Nederlandse universiteiten en laboratoria en onderzoekers uit landen waar de mensenrechten digitaal worden geschonden.

De leden van de CDA-fractie zijn tevens benieuwd naar de rol van satellietverbindingen om het vrije internet in stand te houden. De EU is dit jaar begonnen met de bouw van een eigen netwerk van internet-satellieten om communicatie binnen Europa nog veiliger te maken. Iris2 moet overal in Europa betaalbare internettoegang mogelijk maken en voor beveiligde verbindingen zorgen in geografische gebieden van strategisch belang, zoals het Noordpoolgebied en Afrika. De leden van de CDA-fractie lezen in de Internationale Cyberstrategie niks over deze satellieten en zijn benieuwd welke rol dergelijke satellietverbindingen kan worden toegedicht in het veilig en open houden van het cyberdomein.

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

[1] Zie bijvoorbeeld Nederlands bedrijf levert surveillancetechnologie aan China. (amnesty.nl)

wat er in het Strategische Concept van de NAVO is besloten over de mogelijkheid tot de inwerkingtreding van artikel 5 van de NAVO bij een cyberaanval?

Vragen en opmerkingen van de leden van de SP-fractie

De leden van de SP-fractie hebben kennisgenomen van de Internationale Cyberstrategie. Twee omissies willen deze leden graag benoemen. In de eerste plaats valt het hen op dat er weinig tot geen aandacht wordt besteed aan de macht van de multinationale tech-giganten in het cyberdomein en hoe die macht gebreideld kan worden. Ziet de minister dat ook? Meent de minister dat een verwijzing naar de (vrijwillige) OESO-richtlijnen voldoende is? Er wordt in de strategie gesproken over strategische coalities waarin ook bedrijven zitten. Wordt daarmee big tech bedoeld? Zo niet, welk type bedrijven dan wel?

In de tweede plaats missen de leden van de SP-fractie een herbevestiging van de noodzaak en wenselijkheid van een open overheid en de erkenning van klokkenluiders, ook internationaal. Onder welke pijler van de strategie valt dit? In dit verband nemen de leden van de SP-fractie de gelegenheid te baat om de minister nogmaals te verzoeken om de vrijlating van Julian Assange te bepleiten. Assange is een symbool van de strijd om openheid; de bewering dat zijn onthullingen mensen in gevaar zouden hebben gebracht is tot op heden hol gebleken. De leden van de SP-fractie ontvangen hierop graag een reactie.

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

De leden van de fracties van GroenLinks en PvdA hebben kennisgenomen van de Internationale Cyberstrategie en hebben enkele vragen aan het demissionaire kabinet. De leden van de fracties van GroenLinks en PvdA lezen dat het demissionaire kabinet vasthoudt aan het bestaande standpunt over encryptie, waarmee het demissionaire kabinet aangeeft het niet wenselijk te achten “om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland en sterke encryptie te stimuleren.” Hoe kijkt het demissionaire kabinet naar de wettelijke vastlegging van de bescherming van en het recht op end-to-end encryptie?

De leden van de fracties van GroenLinks en PvdA lezen dat het kabinet zich bewust is van de noodzaak om journalisten te beschermen tegen spionage, intimidatie en vervolging via nieuwe cybertechnologie en restrictief cyberbeleid, zoals internet shutdowns. Welke stappen onderneemt het demissionaire kabinet om journalisten wereldwijd te beschermen tegen spionage-software, zoals Pegasus? De leden van de fracties van GroenLinks en PvdA lezen dat de Internationale Cyberstrategie geen enkele passage bevat over de bescherming van online anonimiteit. Kan de minister aangeven of het demissionair kabinet van mening is dat online anonimiteit beschermd moet worden en, zo ja, hoe het demissionair kabinet hiervoor internationaal op de bres gaat? De leden van de fracties van GroenLinks en PvdA maken zich ten slotte zorgen over polariserende algoritmes op sociale media gebaseerd op clicks en interacties, waarvan we weten dat ze mensen tegen elkaar opzetten en de verspreiding van haat en desinformatie in de hand werken. Welke stappen onderneemt het demissionaire kabinet om deze algoritmes tegen te gaan?

Vragen en opmerkingen van de leden van de ChristenUnie-fractie

De leden van de fractie van de ChristenUnie hebben met belangstelling kennisgenomen van de Internationale Cyberstrategie. Zij hebben daarover nog enkele vragen. In de Internationale Cyberstrategie wordt opgemerkt dat onze nationale veiligheid, ons verdienvermogen en de veilige online omgeving van de burger op dagelijkse basis worden bedreigd door statelijke en criminele actoren. Deze leden zouden graag een overzicht krijgen van de belangrijkste (voorbeelden van) dreigingen waar Nederland daadwerkelijk mee te maken heeft gehad, voor zover dit mogelijk is. In het document wordt ook opgemerkt dat in de huidige geopolitieke context het “multistakeholder-model” onder druk staat, omdat door verschillende staten wordt gepoogd technische discussies te multilateraliseren waardoor betrokkenheid van maatschappelijke organisaties, de private sector, academici en de technische gemeenschap onder druk komt te staan. Dat heeft ook gevolgen voor het model van het beheer van het internet (internet governance). Zou de minister dit nader kunnen toelichten en kunnen aangeven wat de onwenselijke gevolgen hiervan zijn?

De leden van de fractie van de ChristenUnie vragen of de doelstelling om de rol van de EU en de NAVO als internationale cyberactoren te vergroten, de geconstateerde uitdaging dat internationale technische organisaties gepolitiseerd worden, niet verder in de hand zou kunnen werken. Kan de inspraak van de private sector, maatschappelijke organisaties en academici hierdoor juist niet worden beperkt? Ten aanzien van het versterken van de slagkracht in het cyberdomein zouden de leden van de fractie van de ChristenUnie willen weten welke mogelijkheden de minister ziet in het bestaande juridische kader om kwaadwillende actoren en hun facilitators (digitaal) op te sporen, aan te pakken, te verstoren en te vervolgen. Is het kabinet van mening dat er ruimere juridische kaders nodig zouden zijn en, zo ja, op welke punten? Ten aanzien van de inzet van het cybersanctieregime zouden deze leden willen weten wat het vaker inzetten daarvan in de weg staat.

De leden van de fractie van de ChristenUnie vragen of het tegengaan van schadelijke desinformatie, haatspraak en propaganda eigenlijk wel behoort tot het onderwerp cyberveiligheid? Kan het kabinet dit nader onderbouwen? Terecht is er volgens deze leden in de Internationale Cyberstrategie aandacht voor mensenrechten. Zij vinden het ook van groot belang dat mensenrechtenrisico’s van nieuwe technologieën in kaart worden gebracht. Op welke manier gaat het kabinet hier de Kamer van op de hoogte houden? Ook bij het standaardiseringsproces spelen mogelijke risico’s voor mensenrechten en het kabinet wil deze risico’s dan ook nauwlettend in de gaten houden, zo lezen deze leden in de brief. Hoe gaat het kabinet dit doen en hoe wordt de Kamer over de bevindingen geïnformeerd?

Vragen en opmerkingen van de leden van de SGP-fractie

De leden van de SGP fractie hebben met interesse kennisgenomen van de Internationale Cyberstrategie 2023-2028 en stellen daarover graag de volgende vragen. Welke principes acht het kabinet internationaal erkend en welke principes zijn dan juist omstreden? Wat stelt het kabinet voor om te doen aan Providers en Internet Service Providers (ISP’s) die juist niet met politie en justitie werken? Hoe wordt “bulletproof hosting” voorkomen? Het kabinet geeft aan dat het te vroeg is voor een nieuw verdrag over statelijk gedrag in het cyberdomein en dat de toepassing in de praktijk nog echt bekeken moet worden voor een nieuw verdrag. Hoe verlopen

de gesprekken daarover? Wordt er al enige consensus bereikt met gelijkgestemde landen of met Rusland en China? Rusland en China hebben ook een agenda om het tegengeluid in de digitale ruimte tegen te gaan. Dit bemoeilijkt al lang de consensus die nodig zou zijn voor een eventueel nieuw cyberverdrag als opvolger van de Budapestconventie. Hoe ziet het kabinet de mogelijkheid voor consensus en overeenstemming op de lange termijn? En wat zijn de alternatieven voor een breed gedragen verdrag? Wat voor argumenten gebruiken Rusland en China tegen de deelname van niet-statelijke actoren in VN-discussies?

De leden van de SGP-fractie vragen voorts hoe goed Defensie erin slaagt technisch personeel te werven, op te leiden en te behouden voor “cyber readiness” en voor zowel offensieve als defensieve capaciteit om haar rol in deze strategie te vervullen. Welke rol speelt oefening en ervaring in “cyber readiness” en in offensieve en defensieve capaciteit? Hoe werkt Defensie aan die oefening en ervaring? Kan Defensie wellicht een meer ondersteunende rol bieden bij de politie, als dat bijdraagt aan het opdoen van ervaring? Bepaalde statelijke cyberdreigingen worden genoemd in de brief, maar blijven toch buiten bereik van oplossingen. Hoe worden de benoemde vrijhavens bestreden? In de kabinetsbrief lezen de leden van de SGP-fractie over opsporingsmiddelen voor repressiedoeleinden. Wat kan het kabinet in de toekomst doen tegen spionagesoftware? Hoe kijkt het kabinet naar de verspreiding en het gebruik van spionagesoftware?

De leden van de SGP-fractie vragen voorts naar de keuze van het kabinet voor de EU, de NAVO of een samenwerking tussen die twee om internationale cyberdiplomatie te bedrijven. Is er een voorkeur voor een bepaalde partner boven de andere of zijn er duidelijk verschillende inzetten en rollen? Welke middelen heeft het kabinet allemaal in het tegengaan van desinformatie, haatspraak en propaganda? In de brief lezen de leden van de SGP-fractie over “Content Moderation”, die bij platforms zelf is neergelegd. Wat zijn de andere instrumenten? In de strategie lezen zij dat landen soms proberen de technische structuur van het internet naar hun hand te zetten en dat fragmentatie ook dreigt. Hoe verloopt het met deze vraag om erkenning van het niet-politieke karakter van de publieke kern van het internet? Lukt dit in VN-verband al, vragen de leden van de SGP-fractie. En is dat genoeg om de publieke kern en technische structuur van het internet onafhankelijk te laten blijven? Of moeten daar nog vervolgstappen uit voortvloeien? De leden van de SGP-fractie vinden het goed dat het kabinet helpt om Computer Security Incident Response Teams (CSIRT’s) op te bouwen en te versterken in belangrijke partnerlanden en opkomende landen. Hoe verloopt dit? En is dit een doorlopend programma of betreft het tijdelijke ondersteuning, waarna het betreffende land verder gaat?

Vragen en opmerkingen van de leden van de BBB-fractie

De leden van de BBB-fractie hebben kennisgenomen van de Internationale Cyberstrategie 2023-2028. Zij hebben daarover de volgende vragen en opmerkingen. Deze leden zijn het ermee eens dat een pro-actievere omgang met cyberdreigingen nodig is. Ook merken zij op dat de minister een set ‘doorsnijdende beleidsinstrumenten’ voorstelt die een stap in de goede richting zijn met in het bijzonder het versterken van bestaande en nieuwe coalities met opkomende landen. Kan de minister aangeven welke landen zij hieronder zou verstaan en of er ook actief zal worden ingezet op een versterkte cyber-coalitie met bijvoorbeeld digitaal ontwikkelde landen als Taiwan en Israël?

De leden van de BBB-fractie verwelkomen ook het initiatief inzake (extra) investeren in inlichtingencapaciteiten. Wanneer cyberaanvallen op grote bedrijven of ministeries worden uitgevoerd, krijgt het dikwijls nationale aandacht, maar een sluipender probleem is de kwetsbaarheid van lagere overheden en het midden- en kleinbedrijf (MKB) voor cyberaanvallen. Zij hebben vaak niet de middelen, kennis of het digitale bewustzijn om cyberaanvallen te voorkomen of bestrijden. Genoeg financiële en juridische middelen en bevoegdheden voor inlichtingencapaciteiten kunnen bijdragen aan een meer weerbare en efficiëntere nationale cyberveiligheid, aldus de leden van de BBB-fractie. Wat wil het kabinet specifiek ondernemen om lagere overheden en het MKB weerbaarder te maken? Veiligheidsdiensten moeten volgens de leden van de BBB-fractie meer ruimte krijgen om bevoegdheden te gebruiken in hun werk, met daarbij als voorwaarde een wettelijk kader waardoor toezichthouders controles kunnen uitvoeren. Hoe ziet het kabinet een dergelijk juridisch kader?

II Antwoord/ Reactie van de minister

III Volledige agenda

- De brief van de minister van Buitenlandse Zaken van 9 juni 2023 over de Internationale Cyberstrategie (ICS) 2023-2028 (Kamerstuk 26643, nr. 1036).