2017D09582

INBRENG VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Binnen de vaste commissie voor Buitenlandse Zaken bestond bij enkele fracties de behoefte de Minister van Buitenlandse Zaken enkele vragen en opmerkingen voor te leggen inzake de brief d.d. 12 februari 2017 inzake de Internationale Cyberstrategie (Kamerstuk 26 643, nr. 447).

De fungerend voorzitter van de commissie,
Omtzigt

De griffier van de commissie,
Van Toor

Inbreng van de leden van de fractie van de VVD

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de Internationale Cyberstrategie. De VVD-fractie heeft hierover nog enkele vragen en opmerkingen.

In de strategie valt te lezen dat Nederland inzet op wereldwijde capaciteitsopbouw. Kan het kabinet concrete voorbeelden geven van dergelijke capaciteitsopbouw? In welke landen zijn tot nu toe welke specifieke projecten uitgevoerd? Wat was de Nederlandse bijdrage daarbij? En tot welke concrete uitkomsten heeft dat geleid?

In de strategie staat ook dat Nederland actief meewerkt aan het betrekken van ontwikkelingslanden bij het Internet Governance Forum (IGF) en om de resultaten van dit mondiale overlegplatform tastbaarder en zichtbaarder te maken. Kan het kabinet concreet toelichten op welke wijze Nederland daaraan meewerkt? En wat zijn de uitkomsten daarvan toe nu toe?

Onder «verdere versterking cybersecurity» (op pagina 11) wordt gesproken over de versterking van de Europese digitale veiligheid. In het bijzonder gaat de aandacht daarbij uit naar vitale sectoren en infrastructuren. Welke vitale sectoren en infrastructuren identificeert het kabinet binnen de internationale cyberstrategie? Kan het kabinet daar een opsomming met toelichting van geven?

Wat zijn tot nu toe de concrete, praktische opbrengsten van het INTERPOL Global Complex for Innovation (IGCI). Op welke wijze wordt wereldwijde internationale samenwerking in cybercrimezaken ondersteund door het IGCI?

Nederland is voorstander van de ontwikkeling van een Additioneel Protocol bij het Cybercrimeverdrag, waarin de mogelijkheden voor de internationale opsporing van cybercrime verder worden uitgebreid. Kan het kabinet toelichten hoe andere landen in deze kwestie staan? Is een meerderheid van de landen voor of tegen een dergelijk protocol? Welke redenen voeren landen aan die tegen zijn? En op welke termijn acht het kabinet het haalbaar dat een dergelijk Protocol daadwerkelijk tot stand komt?

Waaraan heeft Nederland zich concreet gecommitteerd met de Cyber Defence Pledge? Vloeien hier specifieke verplichtingen uit voort, of maatregelen die Nederland op korte termijn moet nemen inzake cyber, bovenop reeds bestaande plannen? Graag een toelichting.

Kan het kabinet nader toelichten hoe het kabinet de balans probeert te vinden tussen het helpen van andere landen met capaciteitsopbouw op het gebied van cybersecurity enerzijds en het bewaken van strategische nationale veiligheidsbelangen op datzelfde terrein anderzijds?

Inbreng van de leden van de fractie van de PVV

De leden van de PVV-fractie willen het kabinet bedanken voor het naar de Kamer sturen van de Internationale Cyberstrategie. De PVV deelt de mening dat digitale dreigingen één van de grootste veiligheidsdreigingen van deze tijd zijn. De toegenomen aandacht voor dit onderwerp, waarvan de Internationale Cyberstrategie een uitvloeisel is, is daarom meer dan terecht.

Voor de leden van de PVV-fractie moet de bescherming van Nederland, de Nederlandse burgers en bedrijven de spil zijn waaromheen het Nederlands cyberbeleid wordt gebouwd. Zoals het kabinet terecht stelt, neemt de cyberdreiging zowel in kwantiteit als in kwaliteit toe. De leden van de PVV-fractie zijn daarover zeer bezorgd.

De schade die de Nederlandse economie als gevolg van cybercrime en cyberspionage lijdt neemt steeds verder toe. Kan het kabinet een schatting geven van de economische schade die Nederlandse bedrijven en instellingen jaarlijks oplopen? En met welke bedrag neemt deze schadepost naar verwachting toe de komende jaren?

De leden van de PVV-fractie zijn eveneens bezorgd over de dreiging van cyberaanvallen op vitale infrastructuur in Nederland. In welke mate is Nederland daarop voorbereid? Houden de Nederlandse autoriteiten en diensten grootschalige oefeningen waarbij cyberaanvallen op de vitale infrastructuur wordt gesimuleerd?

De leden van de PVV-fractie zijn content met de toegenomen aandacht voor cyberveiligheid bij het NAVO-bondgenootschap en steunen de ontwikkeling van defensieve en offensieve slagkracht in het cyberdomein. Zeker ook daar waar het de maatregelen betreft in bondgenootschappelijk verband. Maar beschikt de Nederlandse krijgsmacht zelf over voldoende personele en materiele cybercapaciteiten? Februari jongstleden gaf de commandant van het Defensie Cyber Commando (DCC) in de media aan dat het DCC nu al overvraagd is. Erkent het kabinet dit zorgelijke beeld, en zo ja, welke maatregelen worden genomen om de ontstane capaciteitstekorten op te lossen in een tijd waarin de werkdruk voor het DCC alleen maar zal toenemen?

Het kabinet gaat een cyberdiplomatennetwerk activeren op enkele belangrijke ambassades. Kan over dit initiatief iets meer helderheid worden verschaft? Wat zijn de tot nu toe opgedane ervaringen en wanneer wordt besloten om het cyberdiplomatennetwerk verder te activeren en uit te rollen op andere ambassades? Ook horen de leden van de PVV-fractie graag of de Nederlandse ambassades extra kwetsbaar zijn voor cybercrime en cyberspionage. Beschikt Nederland wel over voldoende personele capaciteit om staatsgeheimen en andere vertrouwelijke informatie op ambassades uit handen te houden van kwaadwillende hackers?

Tot slot steunen de leden van de PVV-fractie de Nederlandse inspanningen om de internationale opsporing in het cyberdomein te bevorderen. Nu komen cybercriminelen te makkelijk weg met het plegen van criminele daden in het cyberdomein. Dat is de leden van de PVV-fractie een doorn in het oog. Om de opsporing te verbeteren heeft Nederland bijgedragen aan de ontwikkeling van het European Cyber Crime Center bij Europol. Kan het kabinet aangeven in welke mate de oprichting en ontwikkeling van het European Cyber Crime Center heeft bijgedragen aan het opsporen van cybercriminelen? Zijn er al cybercriminelen opgepakt en cyberbendes opgerold met hulp van het European Cyber Crime Center?

Inbreng van de leden van de fractie van D66

De leden van de D66-fractie hebben met belangstelling kennis genomen van de Internationale Cyberstrategie van het kabinet. De genoemde leden onderschrijven het uitgangspunt van het kabinet van een veilig, vrij en open cyberdomein. Digitalisering biedt kansen, maar kent ook vele uitdagingen. Het kabinet stelt terecht dat dit een continue investering vergt en dat hier dus hard voor moet worden gewerkt. De genoemde

leden werken graag samen met het kabinet voor het waarborgen van een vrij, veilig en open cyberdomein.

De leden van de D66-fractie onderschrijven de zorgen van het kabinet over het gebrek aan duidelijke gedragsregels over de inzet van (militaire) cybercapaciteiten. De genoemde leden vinden het dan ook zeer positief dat Nederland deelneemt aan het overleg in de UN Group of Governmental Experts over normen voor een veilig en stabiel cyberdomein. De genoemde leden zouden het op prijs stellen als het kabinet kan delen wat de inzet van Nederland is tijdens dit overleg. Welke concrete afspraken en resultaten streeft het kabinet na? Hoe past de inzet van offensieve cyberwapens, zoals ook in de Nederlandse Defensie Cyber Strategie staat, hier in? Kan het kabinet dit nader toelichten? Kan het kabinet kort, bondig en puntsgewijs uiteenzetten welke gedragsnormen het nastreeft in het cyberdomein?

Belangen en visie

De leden van de D66-fractie onderschrijven de analyse van het kabinet dat in het cyberdomein zowel kansen als dreigingen zijn. Er is sprake van internationale belangen, internationale dreigingen en internationale uitdagingen. Volgens het kabinet zijn veiligheid en vrijheid daarin niet tegengesteld, maar complementair. De genoemde leden vinden dit een interessant uitgangspunt, maar wijzen er tegelijkertijd op dat er wel degelijk een spanning kan bestaan tussen vrijheid en veiligheid. Het is daarom juist noodzaak om de juiste balans te vinden tussen vrijheid en veiligheid. De genoemde leden merken daarbij op dat dit kabinet er vaak voor kiest om privacy op te geven, en daarmee de vrijheid, in een poging de veiligheid te vergroten. Dit gebeurt zowel «offline» door meer cameratoezicht en meer fysieke controles als online met bijvoorbeeld de nieuwe Wet op de inlichtingen- en veiligheidsdiensten waarmee onschuldige mensen makkelijker kunnen worden afgeluisterd. De genoemde leden vragen het kabinet daarom nader uit te leggen wat het bedoelt met de zinsnede dat vrijheid en veiligheid complementair zijn. Hoe zorgt het kabinet er voor dat de balans niet doorslaat naar veiligheid ten koste van vrijheid? Kan het kabinet dit met concrete voorbeelden nader uiteenzetten?

De leden van de D66-fractie zijn het met het kabinet eens dat er talloze internationale dreigingen zijn in het cyberdomein. Die dreigingen komen van zowel statelijke als niet-statelijke actoren. Bovendien kent deze dreiging vele vormen, van zoals cybercrime, cyber-spionage, of zelfs cyber-sabotage. In de huidige analyse van het kabinet missen de genoemde leden een uiteenzetting van de belangrijkste dreigingen voor Nederland. Welke statelijke en niet-statelijke actoren zijn het grootste gevaar voor Nederland en de EU? «Nederland is structureel doelwit van digitale spionageaanvallen», aldus het kabinet. Van wie komen die aanvallen? Wordt dit, waar mogelijk, ook geadresseerd via andere diplomatieke kanalen? Het aantal cyberaanvallen op de VS is na het diplomatieke akkoord tussen China en de VS gedaald. Behoren dergelijke diplomatieke akkoorden ook tot de Nederlandse, en Europese, inzet? Hebben deze aanvallen implicaties voor de Nederlandse Defensie Doctrine en de (Nederlandse) Internationale Veiligheidsstrategie? Zo ja, welke dan? Zo nee, waarom niet?

De leden van de D66-fractie constateren dat het kabinet een verdeling maakt tussen drie groepen landen daar waar het gaat over de mate van vrijheid op internet en toepasbaarheid van internationaal recht. Kan het kabinet bij de analyse ook aangeven wat de krachtsverhoudingen zijn? Hoeveel landen scharen zich achter het standpunt dat ook Nederland

inneemt van een bescherming van de integriteit van het internet en de toepassing van internationaal recht? Zijn dit vooral EU-landen? Welke en hoeveel landen bevinden zich in de andere categorieën van staatsgeoriënteerde landen en *swing states*?

Aanpak

De leden van de D66-fractie merken op dat het kabinet stelt dat maar liefst 5 ministeries direct betrokken zijn bij de aanpak van de Internationale Cyberstrategie. De genoemde leden ontvangen graag een toelichting hoe de afstemming onderling is tussen deze ministeries. Is er een interdepartementale werkgroep? Of gebeurt dit allemaal binnen de Taskforce Cyber die is gelanceerd vanuit Buitenlandse Zaken? En kan het kabinet ook aangeven hoe de verantwoordelijkheidsdeling is? Kan het kabinet dan tevens direct aangeven wat precies de taak- en functieomschrijving is van de Speciaal Gezant voor internationaal cyberbeleid die door Buitenlandse Zaken is aangesteld? Welke dagelijkse belangrijke werkzaamheden onderneemt deze Speciaal Gezant die zijn positie rechtvaardigen? Met andere woorden: waarom is een dergelijk Speciaal Gezant nodig?

De leden van de D66-fractie vragen het kabinet toe te lichten, indien mogelijk, hoe vaak offensieve cybercapaciteiten door Nederland zijn en worden ingezet? Gebeurt dit op dagelijkse basis? Of zijn dit gerichte aanvallen die slechts sporadisch plaatsvinden? Kan het kabinet in dit verband ook aangeven hoe het omgaat met het recht op informatie (inlichtingen) vooraf van de Staten-Generaal bij de inzet of het ter beschikking stellen van de krijgsmacht?

De leden van de D66-fractie hebben met belangstelling kennis genomen van de aangekondigde ontplooiing van een cyberdiplomatennetwerk voor het Nederlandse cyberbeleid, beginnend op een aantal belangrijke ambassades. De genoemde leden zouden het zeer op prijst stellen als het kabinet dit nader kan toelichten. Welke concrete rol krijgen deze cyberdiplomaten? Welke en hoeveel middelen zijn hiervoor beschikbaar? Zijn dit nieuwe voltijdsfuncties, waarvoor experts worden aangetrokken? Of krijgen de huidige diplomaten er een extra taak bij? Wat is de precieze taak- en functieomschrijving van deze cyberdiplomaten? En op welke ambassades gaan zij aan het werk?

De leden van de D66-fractie constateren dat het kabinet vooral inzet op repressieve veiligheidsmaatregelen in plaats van preventie, terwijl juist op het gebied van preventie nog een wereld te winnen is. Een groot deel van de wereldwijde cybercrime is het gevolg van onveilige software, slechte cyberhygiëne en onvoldoende bewustzijn. Hier ligt ook de focus van de initiatiefnota van de D66-fractie over veilige op internet aangesloten apparaten. Bijvoorbeeld door bedrijven aan te spreken op hun verantwoordelijkheid, bijvoorbeeld door middel van software aansprakelijkheid, door mensen en bedrijven te ondersteunen in goede cyberhygiëne en door het bewustzijn bij mensen, bedrijven en overheden te vergroten. Kan het kabinet aangeven hoe het aankijkt tegen het belang van preventie? Welke stappen is het van plan op dit gebied, ook in Europese en internationale context, te nemen?

Beleidsprioriteiten van een internationale cyberstrategie

De leden van de D66-fractie constateren dat het kabinet voor een effectieve bestrijding van cybercrime vooral inzet op intensivering van de internationale samenwerking en het versterken van internationale juridische kaders. Graag ontvangen de genoemde leden ook een

toelichting of, en zo ja welke, capaciteit in Nederland wordt ontwikkeld om internationale cybercrime op te sporen en aan te pakken.

De leden van de D66-fractie constateren dat de juridische experts die aan de basis staan van de Tallinn Manual 2.0 er onderling niet uit kunnen komen wat betreft de legaliteit van buitenlandse cyberspionage. Op pagina 170 stellen zij: « [we] were incapable of achieving consensus as to whether remote cyber espionage reaching a particular threshold of severity violates international law». Wat is de mening van het kabinet hierover? Hoe verhoudt zich deze uitspraak in de Tallinn Manual 2.0 met de verruiming van de bevoegdheden in de Wet op de Inlichtingen- en veiligheidsdiensten?

De leden van de D66-fractie lezen dat het kabinet andere landen wil bewegen tot transparantie over offensieve cybercapaciteiten. Welke landen erkennen op dit moment dat zij offensieve cybercapaciteiten hebben, ontwikkelen en/of inzetten? En van welke landen heeft het kabinet het vermoeden dat dit zo is, en zijn de betreffende landen daar dus niet transparant over?

De leden van de D66-fractie constateren dat investeringen in offensieve cybercapaciteiten tevens negatieve gevolgen kunnen hebben voor defensieve cybercapaciteiten. Het opsparen en het openlaten van kwetsbaarheden in veelgebruikte consumentensoftware kan voor de samenleving negatieve gevolgen hebben op het gebied van economie, privacy en veiligheid. Erkent het kabinet deze dualiteit in de ontwikkeling van offensieve cybercapaciteiten? Hoe houdt het kabinet rekening met deze dualiteit in de ontwikkeling van offensieve cybercapaciteiten? Hoe verloopt de afweging tussen de offensieve mogelijkheden enerzijds en de defensieve risico's anderzijds? Hoe verloopt de inschatting van de defensieve risico's van het openlaten van kwetsbaarheden in veelgebruikte consumentensoftware? Kan het kabinet een voorbeeld geven van een doel van de offensieve cybercapaciteiten waarover transparantie dient te bestaan volgens het kabinet?

Inbreng van de leden van de fractie van GroenLinks

De leden van de fractie van GroenLinks hebben met belangstelling de Internationale Cyberstrategie gelezen. Zij kunnen zich vinden in de uitgangspunten, maar vinden de strategie op veel vlakken nog weinig concreet. Gezien het portefeuille-overstijgende karakter en ook het grote belang van het internet, hechten de leden aan een heldere verdeling van taken en bevoegdheden tussen bewindspersonen en tussen diensten. Is er op dit moment een helder beeld van de rollen van de ministers van Buitenlandse Zaken, Defensie, Veiligheid & Justitie, Economische Zaken en Binnenlandse Zaken en de onder hen ressorterende diensten op dit terrein? Acht het kabinet het raadzaam om in een volgend kabinet een coördinerend bewindspersoon aan te wijzen?

Aanpak

Hoe worden op dit moment aanvallen die aan statelijke actoren worden toegeschreven, tegemoet getreden? Welke acties worden ondernomen als er een redelijk vermoeden bestaat dat een andere staat verantwoordelijkheid draagt, bijvoorbeeld voor pogingen tot beïnvloeding van verkiezingen of digitale spionage? Bestaat er steun voor het opstellen van een internationaal juridisch kader? Wat is de officiële visie van Rusland en China op dergelijke interstatelijke aanvallen? Zijn landen verantwoordelijk voor het berechten van cybercriminelen die op hun grondgebied opereren en voor het verhalen van de schade die deze cybercriminelen toebrengen?

Wat verstaat het kabinet onder robuuste capaciteiten? Beschikt de overheid, en met name het Nationaal Cyber Security Centrum (NCSC), over voldoende gekwalificeerde mensen? Wat is de invullingsgraad van de vacatures bij het NCSC? Loopt het opbouwen van capaciteiten gelijk op met het toenemen van de dreiging? Wat zijn de financiële kaders van de cybercapaciteit van de Nederlandse overheid?

Wat zijn de taken van het cyberdiplomatennetwerk? Wordt de cyberportefeuille onderdeel van het werk van zittende diplomaten of worden hiervoor gespecialiseerde diplomaten uitgezonden? Hoe verhoudt dit netwerk zich tot de NCSC?

De leden van de fractie van GroenLinks onderschrijven het belang van het integreren van het cyberbeleid in het gemeenschappelijk buitenland- en veiligheidsbeleid. Zijn er concrete plannen om deze integratie door te voeren? Hoe staan de Europese Dienst voor Extern Optreden (EDEO), de Europese Commissie en de lidstaten hier tegenover?

Beleidsprioriteiten

Wie maken deel uit van de Samenwerkingsgroep? Zijn de EU-lidstaten bereid om in het kader van cyberbeleid samen op te trekken? Of betreft het hier meer een voorhoede onder de lidstaten?

Wie is verantwoordelijk voor de samenwerking tussen de Computer Security Incident Response Teams (CSIRTs)?

Waar liggen de grenzen tussen de militaire en civiele componenten van cybercapaciteiten? Heeft het kabinet het in het kader van NAVO over de cybercomponent van militaire operatie of heeft de NAVO een bredere rol? Hoe verhoudt de rol van de NAVO zich tot de rol van de EU? Committeren de verschillende NAVO-partners zich aan een bondgenootschappelijke houding? Hoe ziet het kabinet in dit kader de eerdere berichten over het afluisteren van de Duitse bondskanselier door de Amerikaanse inlichtingendienst CIA en over Turkse spionage van Turkse Duitsers in Duitsland? Is er voldoende vertrouwen om cybercapaciteiten in NAVO-verband op te bouwen?

Met welke intentie wil de Europese Commissie de Dual-Use Verordening uitbreiden? Waarom is het kabinet hier uiterst kritisch over? Over welk gelijk speelveld maakt het kabinet zich zorgen? Is het kabinet bezorgd dat Europese bedrijven minder gespecialiseerde software aan autoritaire regimes kan leveren als de verordening herzien wordt? Hoe verhoudt dit zich tot de focus van het kabinet op mensenrechten?

Inbreng van de leden van de fractie van de SP

De leden van de SP-fractie hebben kennis genomen van de Internationale Cyberstrategie en hebben daarover een aantal vragen en opmerkingen, vooral betreffende internationale vrede, veiligheid en stabiliteit.

In de Cyberstrategie schrijft het kabinet dat verschillende kwaadwillende actoren steeds meer gebruik maken van het cyberdomein om hun belangen na te streven, onder andere voor politiek-militaire doeleinden. De leden van de SP-fractie vragen het kabinet aan te geven waar deze dreiging voor Nederland vandaan komt. Welke landen zijn hier met name verantwoordelijk voor en in hoeverre is duidelijk in welke mate de kwaadwillende actoren gelinkt kunnen worden aan de autoriteiten in de desbetreffende staten?

Omdat de dreiging in het cyberdomein toeneemt, zijn er extra capaciteiten nodig om dit te bestrijden. Hoeveel capaciteit, financieel, maar ook wat fte's betreft, er in de afgelopen tien jaar bijgekomen is om deze dreiging tegen te gaan?

Een groot probleem bij cyberaanvallen is dat de oorsprong van de aanval soms moeilijk te achterhalen is. De leden van de SP-fractie vragen de Minister hier nader op in te gaan. Klopt het dat het soms niet mogelijk is te achterhalen wie er achter een cyberaanval zit? Welke problemen bestaan er op dit vlak? Kan het kabinet in dit verband ook reageren op de geheime documenten die onlangs door WikiLeaks werden geopenbaard, vooral wat betreft de mogelijkheden waarover de CIA zou beschikken om cyberaanvallen te verhullen van de VS en juist de indruk te wekken dat een ander land achter bijvoorbeeld een hackpoging zit? Kan het kabinet ook meer in het algemeen toelichten welke mogelijkheden er zijn om in het geval van een cyberaanval de indruk te wekken dat een ander land verantwoordelijk is?

De leden van de SP-fractie vragen het kabinet ook meer in het algemeen te reageren op de recente onthullingen dat de CIA over mogelijkheden beschikt om onder meer via telefoons, televisies en laptops mensen af te luisteren. In hoeverre is daardoor de privacy in gevaar? Op welke schaal gebeurt dit reeds? Is hierover contact met de Amerikanen? Kan ook gereageerd worden op de onthulling dat de CIA zelfs de besturing van zogenaamde smart auto's over zou kunnen nemen? Kan dat bevestigd worden? Gebeurt dit reeds in de praktijk? Verwerpt het kabinet dergelijke praktijken? Hoe wordt hiertegen geprotesteerd? In hoeverre kan het schrikbeeld dat George Orwell in zijn boek 1984 beschreef met de technieken waarover de CIA kennelijk beschikt, bewaarheid worden?

In de Cyberstrategie verwijst het kabinet naar de mogelijke rol van Rusland in de hacks tijdens de Amerikaanse verkiezingen. De leden van de SP-fractie vragen of toegelicht kan worden in hoeverre er nu meer duidelijkheid bestaat over de mogelijke Russische betrokkenheid hierbij. Heeft het kabinet enig bewijs gezien dat Rusland verantwoordelijk is? De Amerikaanse Senator McCain heeft deze hacks een oorlogsdaad genoemd. Deelt het kabinet die analyse?

In politiek en media is vooral aandacht voor toenemende aanvallen via het internet op Nederland en andere westerse landen vanuit China, Rusland en Iran. De zorgen hierover worden door de leden van de SP-fractie gedeeld. Veel minder aandacht is er voor cyberaanvallen vanuit het westen, met name vanuit de VS. Kan het kabinet hier nader op ingaan? Zijn voorbeelden bekend van cyberaanvallen door de VS, bijvoorbeeld op Rusland, China en Iran? Deelt het kabinet de opvatting van menig analist dat de Stuxnetaanval in 2010 een Amerikaanse aanval, wellicht met Israëlische steun, op Iran was? Zo nee, welke analyse is er dan van deze cyberaanval gemaakt? Hoe verhoudt de omvang en kwaliteit van cyberaanvallen vanuit het westen zich, grofweg, tot cyberaanvallen tegen westerse landen?

De leden van de SP-fractie hebben heel grote zorgen over toenemende cyberaanvallen, niet in de laatste plaats omdat dergelijke aanvallen grote schade kunnen aanrichten aan de civiele infrastructuur en het mogelijk is dat deze uitmonden in een gewapend conflict. Deelt het kabinet deze zorgen? Welke bereidheid bestaat er in westerse en andere landen om duidelijke regelgeving overeen te komen om de cyberaanvallen aan banden te leggen? Waarom gebeurt dit tot op heden onvoldoende?

Nederland ontwikkelt offensieve cyberslagkracht zodat, indien nodig, geïntervenieerd kan worden. De leden van de SP-fractie hebben hier grote zorgen over. Kan het kabinet de precieze juridische beperkingen aangeven voor het inzetten van een cyberaanval? Is een cyberaanval alleen mogelijk als reactie op een aanval vanuit een ander land? Is het uitgesloten dat een cyberaanval wordt ingezet buiten de context van een gewapend conflict? Kan ook toegelicht worden onder welke omstandigheden een cyberaanval gekwalificeerd kan worden als een oorlogsdaad?

In de cyberstrategie staat dat er gestreefd wordt naar transparantie, maar niet over de aard van de cybercapaciteiten. De leden van de SP-fractie vragen waarom hier niet meer helderheid over verschaft kan worden. Het kabinet pleit voor meer transparantie over de doelen waar de cybercapaciteiten toe dienen, het juridische kader waaronder zij worden ingezet en de politieke controle en het democratisch toezicht op de inzet daarvan. Kan het kabinet op al deze punten zelf ook meer transparantie bieden?

Nederland zoekt naar coalities met gelijkgestemde landen om het recht op bescherming van persoonsgegevens en het recht op privacy te behartigen. De leden van de SP-fractie vragen het kabinet aan te geven of het hier ook coalities betreft met de VS. Zo ja, kan dan toegelicht worden hoe de VS, na alle onthullingen over afluisterpraktijken door Amerikaanse inlichtingendiensten, waaronder van Europese politici, een gelijkgestemd land kan zijn?

Inbreng van de leden van de fractie van de PvdA

De leden van de PvdA-fractie hebben met belangstelling kennis genomen van de Internationale Cyberstrategie van het kabinet. De genoemde bedreigingen komen van veel kanten, raken verschillende belangen en doelen. Het is daarom goed dat deze bedreigingen inclusief de betrokken nationale en internationale partijen die daar tegen strijden in onderlinge samenhang worden gebracht. Deze leden hebben nog enkele vragen en opmerkingen.

Zo lezen de leden van de PvdA-fractie dat aan de ene kant Nederland baat heeft bij een open, ongefragmenteerd internet waarbij informatie vrij kan bewegen, maar aan de andere kant lezen deze leden ook dat gestreefd wordt naar internationale gedragsnormen en -afspraken. Hoe verhoudt het een zich tot het ander? Is het mogelijk dat de zelforganisatie en -regulering waardoor internet tot een wereldwijd gedeelde en voor iedereen toegankelijke infrastructuur kon groeien, door die gedragsnormen en afspraken beperkt gaat worden? Zo ja, wat zullen de gevolgen daarvan zijn? Zo nee, waarom niet? Wat is de stand van zaken betreffende het door Nederland bij de VN ingediende initiatiefvoorstel over internationale gedragsregels en normen?

Biedt de nieuwe Wet op de inlichtingen- en veiligheidsdiensten, op het moment dat die in werking zou treden, betere mogelijkheden om tegen cyberbedreigingen vanuit het buitenland op te treden dan de huidige wet? Zo ja, op welke wijze?

De leden van de PvdA-fractie lezen op meerdere plaatsen in de Cyberstrategie dat de grenzen van het recht, die meestal tot de nationale grenzen beperkt blijven, niet passen bij het grensoverschrijdende karakter van het internet. Zo zouden criminelen er van profiteren dat het traditionele systeem waarbij landen elkaar rechtshulpverzoeken doen te traag werkt en de criminelen daardoor als het ware snel kunnen ontsnappen. Trekt het kabinet hier conclusies uit? Of ziet het kabinet het als een gegeven dat de klassieke jurisdictie van nationale staten nu eenmaal niet passend is in de

strijd tegen cybercrime? De leden van de PvdA-fractie lezen dat de Europese Commissie in ieder geval laat uitwerken welke aanknopingspunten er mogelijk zijn «voor handhavingsjurisdictie anders dan territorialiteit, en of er opsporingsbevoegdheden zijn die onafhankelijk van territoriale grenzen gebruikt kunnen worden». Is er al zicht op waar de Commissie daarbij aan denkt? Zo ja, wat hoe ziet de Commissie deze jurisdictie buiten de nationale grenzen voor zich? Zo nee, op welke termijn valt dit wel te verwachten?

Ook wijst het kabinet op het feit dat de anonimiteit van het internet en het decentrale karakter daarvan «een belangrijke uitdaging» vormen voor een effectief internationaal beleid. Hoe moeten de leden van de PvdA-fractie dit duiden? Hoe wil het kabinet die effectiviteit in dit verband toch vergroten? Gaat dat alleen via de weg van vrijwilligheid en overreding van landen die minder dan Nederland op het internationaal recht georiënteerd zijn? Of ziet het kabinet ook mogelijkheden om internationaal tot dwingender afspraken te komen? Zo ja, op welke manier?

Hoe moeten de leden van de PvdA in dit verband de rol van bedrijven zien waarvan het kabinet van mening is dat die vanwege hun wereldwijde dominante marktpositie ook negatieve invloed kunnen hebben? Worden met deze bedrijven afspraken gemaakt, die eventueel internationaal gelden, om te voorkomen dat die bedrijven misbruik maken van hun dominante marktpositie? Aan welke bedrijven denkt het kabinet in dit kader concreet?

Wat is de stand van zaken van het cyberdiplomatennetwerk dat het kabinet gaat activeren?

De leden van de PvdA-fractie lezen (p. 12 van de Cyberstrategie) dat er sprake is van een Europees netwerk van openbaar aanklagers om de internationale samenwerking voor opsporing in het cyberdomein te verbeteren. Het besluit tot dat netwerk werd in juni 2016 genomen. Wat is de stand van zaken?