Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 418

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 25 augustus 2016

De vaste commissie voor Buitenlandse Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Buitenlandse Zaken over de brief van 19 mei 2016 over de kabinetsreactie op het advies nr. 92 «Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht» van de Adviesraad Internationale Vraagstukken (AIV) en het advies nr. 94 «De publieke kern van het internet: naar een buitenlands internetbeleid» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) (Kamerstuk 26 643, nr. 411).

De vragen en opmerkingen zijn op 23 juni 2016 aan de Minister van Buitenlandse Zaken voorgelegd. Bij brief van 22 augustus 2016 zijn de vragen, mede namens de ministers van Binnenlandse Zaken en Koninkrijksrelaties, van Economische Zaken en van Defensie en de Staatssecretaris van Veiligheid en Justitie, beantwoord.

De voorzitter van de commissie,
Eijsink

De griffier van de commissie,
Van Toor

kst-26643-418
ISSN 0921 - 7371
's-Gravenhage 2016

Inbreng van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met interesse kennisgenomen van de kabinetsreactie op het advies nr. 92 «Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht» van de Adviesraad Internationale Vraagstukken (AIV) en het advies nr. 94 «De publieke kern van het internet: naar een buitenlands internetbeleid» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR). De VVD-fractie heeft hierbij nog enkele vragen en opmerkingen.

Internationale samenwerking

De leden van de VVD-fractie onderschrijven de noodzaak van internationale samenwerking teneinde de veiligheidsuitdagingen op het internet te lijf te gaan. Het kabinet schrijft dat daarvoor internationale samenwerking vereist is, «zoals binnen de EU, VN en Raad van Europa». Deze leden begrijpen dat cybersecurity in deze drie fora kan worden besproken, maar uit de kabinetsreactie wordt niet duidelijk hoe de verantwoordelijkheidsverdeling is geregeld en in hoeverre het gesprek over cybersecurity verschilt per forum. De genoemde leden vernemen graag wat bijvoorbeeld de rol van de Raad van Europa kan zijn op dit vlak. Daarnaast zijn deze leden benieuwd of de NAVO bewust niet in de rijtje wordt genoemd, en of het kabinet onderschrijft dat samenwerking op het gebied van cybersecurity misschien wel het belangrijkst is in NAVO-verband.

I. Antwoord van het Kabinet:
Het grensoverschrijdende en mondiale karakter van het internet vereist dat uitdagingen op het gebied van veiligheid ook internationaal aangepakt worden. Nederland werkt daarom op het gebied van cybersecurity internationaal samen binnen de EU, de VN, de NAVO, de OVSE en de Raad van Europa (RvE).

Elk forum heeft zijn eigen rol in het verbeteren van de cybersecurity in de breedste zin van het woord. Vaak omvatten cyberdreigingen in de praktijk meerdere van de in de rapporten genoemde veiligheidsdimensies en soms hebben ze ook betrekking op meerdere fora. Hierdoor is het noodzakelijk dat de departementen en uitvoeringsorganisaties elkaar doorlopend informeren en de Nederlandse inzet met elkaar afstemmen, zodat deze in de internationale fora coherent, helder en effectief is.

Zonder in details te treden, kunnen we stellen dat een aantal fora zich bezig houdt met een aantal duidelijk te identificeren taken. De bestrijding van cybercrime wordt in het kader van de Raad van Europa en de EU besproken. De Raad van Europa ondersteunt de uitvoering van het Cybercrimeverdrag uit 2001 en faciliteert in dat kader het overleg over onder meer internationale samenwerking, capaciteitsopbouw en de uitvoering van het verdrag. De VN tracht vrede en veiligheid te bevorderen o.a. door middel van de United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) waarin Nederland in 2016–2017 plaats zal nemen. Tot slot wordt binnen de NAVO met behulp van het principe van collectieve verdediging de veiligheid van de bondgenoten gewaarborgd. Dit principe geldt ook voor het cyberdomein.

In het kader van de discussie over cyberveiligheid, en in het bijzonder over cyberwarfare, zijn de leden van de VVD-fractie tevens benieuwd wat de laatste ontwikkelingen zijn op het gebied van de discussie over

cyberwarfare en artikel 5 van het NAVO-Handvest. Dit is eerder in diverse overleggen met de Minister van Defensie aan de orde geweest. Deze leden vernemen graag of er de afgelopen tijd nog beweging heeft gezeten in deze discussie.

II. Antwoord van het Kabinet:
Zoals vermeld in de voortgangsrapportage van de Defensie Cyber Strategie van begin dit jaar (Kamerstuk 33 321, nr. 7 van 15 maart 2016) is het Defensie Cyber Commando opgericht om operationele cybercapaciteiten voor de ondersteuning van militaire missies op te bouwen en de inzet ervan te coördineren. Operationele digitale middelen bestaan uit het geheel van de kennis, de middelen en het conceptuele kader om in een militaire operatie het handelen van tegenstanders te voorspellen, te beïnvloeden of onmogelijk te maken. Ook het vermogen eigen eenheden tegen vergelijkbaar handelen door een tegenstander te beschermen is onderdeel van de operationele cybercapaciteit. Operationele digitale middelen bevatten dus defensieve, offensieve en inlichtingenelementen. Het Joint IV Commando ondersteunt de operationele commandant primair bij de uitvoering van de defensieve taken. Op inlichtingengebied wordt hoofdzakelijk gebruikgemaakt van de MIVD. De komende periode besteedt Defensie nadrukkelijk aandacht aan het inzichtelijk maken van de mogelijkheden die het cyberdomein biedt voor operaties. Bewust nadenken over de kansen en bedreigingen in het cyberdomein, als onderdeel van het planningsproces en in militaire oefeningen, vergroot dit inzicht.

Tijdens de NAVO-top in Wales in september 2014 is uitgesproken dat het internationaal recht ook van toepassing is op het cyberdomein en dat een ernstig cyberincident kan worden bestempeld tot zaak voor de alliantie op grond van artikel 5 van het NAVO-handvest. Indien er geen sprake is van een artikel 5-situatie is NAVO's huidige beleid beperkt tot het verdedigen van de eigen netwerken. Dat verhoudt zich echter niet meer tot de zeer brede inzet van cybermiddelen door potentiële opponenten, zoals spionage, propaganda, maar eventueel ook in een operationele context door middel van sabotage en destructie. Om deze realiteit te erkennen en deze dreiging het hoofd te bieden, wordt cyberspace tijdens de aanstaande NAVO-top in Warschau erkend als operationeel domein, zoals dat al het geval is voor de domeinen land, zee en lucht. Nederland erkent reeds sinds 2012 cyberspace als militair domein. Door de erkenning van het cyberdomein als operationeel domein door NAVO zal cyberverdediging in het volledige operationele proces worden geïntegreerd. Door deze erkenning wordt het ook mogelijk om binnen de NAVO de discussie te openen over het ter beschikking stellen van nationale operationele capaciteiten van bondgenoten ten behoeve van de collectieve verdediging of NAVO missies en operaties. Naast de technische verdediging van de netwerken, wordt het cyberdomein bijvoorbeeld voortaan ook meegenomen in het opstellen van dreigingsbeelden en bij het plannen van een operatie. NAVO's taken en verantwoordelijkheden in het cyberdomein worden hierdoor verder genormaliseerd, waarbij de primaire focus verschuift van het beschermen van de NAVO-netwerken naar de bescherming van NAVO-missies en -operaties.

De leden van de VVD-fractie worstelen nog met twee onderdelen in de kabinetsreactie die moeizaam samen lijken te gaan. Enerzijds onderschrijft

het kabinet constant de noodzaak van internationale samenwerking en de noodzaak van een internationale strategie. Anderzijds constateert het kabinet dat het bijzonder moeizaam blijkt om overeenstemming te vinden, bijvoorbeeld blijkens de onderhandelingen over de eindverklaring van de *World Summit on Information Society (WSIS) +10 Review Process*, waar in het slotdocument enkel de beginselen uit de in 2005 overeengekomen Tunis Agenda zijn herbevestigd. In dat licht vragen de genoemde leden zich af hoe het kabinet hiermee omgaat. Hoe zinvol zijn de inspanningen, bijvoorbeeld in VN-verband, als telkens weer blijkt dat buitengewoon veel landen een geheel andere visie hebben op de rol van de overheid in het cyberdomein? Noopt deze realiteit niet tot samenwerking in kleinere verbanden, opdat overeenstemming makkelijker wordt bereikt?

III. Antwoord van het Kabinet:
Het kabinet beseft dat er in het internationale debat aanzienlijke verschillen zijn in visie op het digitale domein. Nederland zoekt daarom naar kleinere coalities met gelijkgestemden, maar neemt waar mogelijk ook deel aan bredere coalities met gelijkgestemde landen, swing-states en andersdenkenden. Daarnaast wordt in multistakeholder verband ook samengewerkt met niet-statelijke actoren.
Het kabinet is van mening dat onderhandelingen in een breed verband, samenwerking in kleinere verbanden niet uitsluiten. Zo consulteerde Nederland in breed verband tijdens «the Hague Process» met meer dan 50 staten over de toepassing van internationaal recht in cyberspace, en werd in kader van the Global Conference on Cyberspace met een grote groep landen gewerkt aan een vrij, open en veilig internet. Ook in kleinere verbanden zoals in de OVSE, de UN GGE en de Freedom Online Coalitie wordt er gediscussieerd over maatregelen om het internet vrij, open en veilig te houden.

Interdepartementale coördinatie

Het kabinet schrijft dat er een coördinatiestructuur is opgezet voor standpuntbepaling en besluitvorming, op het gebied van cyber security. Kan het kabinet aangeven hoe het deze structuur heeft vormgegeven? Betreft het een interdepartementale werkgroep? Of is de samenwerking van diverse beleidsafdelingen op een meer informele manier versterkt? Leidt dit tot niet tot de gebruikelijke Haagse verkokering? En is overwogen om een heldere, afgebakende eenheid te creëren met doorzettingsvermogen onder één Minister?

IV. Antwoord van het Kabinet:
Het kabinet staat op het standpunt dat de interdepartementale coördinatiestructuur voor standpuntbepaling niet leidt tot verkokering. De Nationale Cyber Security Strategie 2 constateerde in 2013 al dat een gezamenlijke inspanning van alle betrokken publieke partijen als ook private partners benodigd is, waarbij eenieder zijn eigen verantwoordelijkheid moet nemen. De verantwoordelijkheden zijn binnen de rijksoverheid daarom helder belegd. De departementen zoals genoemd in paragraaf 3.3 van de kabinetsreactie zijn verantwoordelijk voor het coördineren van afstemming op relevante dossiers. De vorm van interdepartementale (rijksbrede en publiek-private) coördinatie van de internationale inbreng is afhankelijk van het dossier in kwestie. Soms gebeurt dit in vaste (schriftelijke) gremia, zoals in het tweemaandelijkse Directeuren Overleg Cyber Security (DOCS), ondersteund door het Interdepartementale Overleg Cyber

Security (IOCS), en soms gebeurt dit ad hoc zoals bij de bepaling van het kabinetsstandpunt inzake encryptie.

Nederlandse inzet

Het kabinet schrijft dat Nederland samen met Senegal aan cybersecurity-strategieën voor West-Afrika werkt. Eerder in de kabinetsreactie schreef het kabinet «dat het internationaal cyberbeleid gebaseerd dient te zijn op de nationale belangen van Nederland». Kan het kabinet in het licht van die opmerking aangeven welk belang Nederland heeft bij het uitwerken van cybersecurity-strategieën voor West-Afrika?

V. Antwoord van het Kabinet:
Door het grensoverschrijdende internet vervaagt het onderscheid tussen binnenlands en buitenlands veiligheidsbeleid. Nederland investeert in digitale veiligheid in derde landen om te voorkomen dat cyberdreigingen ontstaan die ook in Nederland schade kunnen berokkenen. Een betrouwbare digitale omgeving in derde landen is ook in het belang van het Nederlandse bedrijfsleven, dat hier een groeiende afzetmarkt voor haar digitale producten en cybersecuritydiensten vindt.

In het Global Forum on Cyber Expertise (GFCE) worden initiatieven voor het delen van kennis en kunde over digitale veiligheid samengebracht. Hieronder vallen het ontwikkelen van cybersecuritystrategieën (onder andere in Afrika), het versterken van de positie van internetnooddiensten en het aanmoedigen van de samenwerking met ethische hackers. De leden van het GFCE onderschrijven de Nederlandse principes van een vrij, open en veilig internet. Nederland heeft als voorzitter van het Global Forum on Cyber Expertise een sterke en zichtbare rol.

Nederland heeft als eerste land een vooruitstrevende aanpak ten aanzien van ethische hackers gerealiseerd met het formuleren van de Responsible Disclosure richtlijn uit 2013. Dit wordt internationaal uitgedragen tijdens relevante momenten, zoals de Global Conference on Cyberspace in 2015 en tijdens het EU-voorzitterschap. Een zichtbaar resultaat van deze inzet zijn de 28 multinationals die zich tijdens de hoogambtelijke bijeenkomst cybersecurity in mei 2016 onder het Nederlands voorzitterschap hebben gecommitteerd aan het Coordinated Vulnerability Disclosure manifest.

Nederland ambieert volgens het kabinet een leidende rol als *digital gateway to Europe* en tevens als *safe place to do business and for people*. Het kabinet verwijst in deze paragraaf naar het lopende Nederlandse EU-voorzitterschap. Kan het kabinet aangeven wat Nederland, nu het EU-voorzitterschap bijna afgerond is, concreet heeft bereikt op het gebied van cybersecurity, cyber crime en andere digitale zaken?

VI. Antwoord van het Kabinet:
Uw Kamer is apart geïnformeerd over de resultaten van het Nederlands voorzitterschap in de brief *Resultaten en uitvoering van het Nederlandse EU-voorzitterschap* d.d. 7 juli 2016 (Kamerstuk 34 139, nr. 18)) en de brief *Overzicht van de resultaten van het Nederlands Voorzitterschap op de JBZ-terreinen Veiligheid en Justitie en Asiel en Migratie* d.d. 5 juli 2016 (Kamerstuk 32 317, nr. 433).

Het versterken van cybersecurity evenals het bestrijden van cybercrime in de EU was een van de prioriteiten voor het kabinet tijdens het voorzitterschap. Deze prioriteit is zowel op politiek als ambtelijk niveau vormgegeven met het doel om bewustzijn over de toenemende dreiging en afhankelijkheid van informatie en communicatie technologie (ICT) te verhogen en de opsporing op internet te versterken.

Nederland zal blijven monitoren dat dat de opbrengst van het voorzitterschap zowel door de Raad als de Europese Commissie wordt verder gebracht.

Inbreng van de leden van de PvdA-fractie

De leden van de PvdA-fractie danken het kabinet voor de kabinetsreactie. Zij hebben een aantal vragen en opmerkingen.

In de kabinetsreactie op het AIV advies nr. 92 «Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht» en het WRR advies nr. 94 «De publieke kern van het internet: naar een buitenlands internetbeleid» lezen de leden van de PvdA-fractie dat het kabinet constateert dat Nederland al belangrijke stappen heeft gezet om maximaal te kunnen profiteren van de kansen die het internet biedt en de rapporten van de AIV en de WRR ziet als een aansporing om de ingezette koers te handhaven en te versterken. Ook lezen de leden van de PvdA-fractie dat het Nederlandse kabinet inzet op een vrij, open en veilig internet. De leden van de PvdA-fractie zijn het met het kabinet eens dat een vrij, veilig en open internet gewaarborgd moet worden. Zij vinden de reactie van het kabinet op de twee adviezen echter weinig concreet en hebben een aantal vragen over hoe het handelingsperspectief waar het kabinet over spreekt, zal worden vormgegeven.

Zo lezen de leden van de PvdA-fractie dat het Nederlandse *internet governance* model tot doel heeft de ontwikkeling, de openheid, de beschikbaarheid, de betrouwbaarheid en de integriteit van het internet te waarborgen. De leden van de PvdA-fractie zien dat het beleid van het kabinet op een aantal punten niet helemaal aansluit bij dit doel. Een belangrijk advies uit het WRR-rapport is dat er een internationale norm moet worden vastgelegd waarin de centrale protocollen van het internet aangemerkt worden als een neutrale zone. In deze zone is bemoeienis omwille van eigen nationale belangen niet geoorloofd.

Er is vanuit het kabinet weinig aanzet tot uitwerking van de voorstellen uit het WRR-advies terug te vinden. Ten eerste de status van het Domain Name System (DNS) en kernprotocollen, waaronder de protocol suite of Transmission Control Protocol/Internet Protocol (TCP/IP) suite. De leden van de PvdA-fractie zouden graag zien dat DNS en de kernprotocollen een speciale status krijgen en daarmee extra bescherming tegen ingrepen door de eigen en andere overheden. Is het kabinet bereid hier naar te kijken? In de kabinetsreactie wordt enkel gesproken over TCP/IP, maar in het WRR-advies is de publieke kern veel breder gedefinieerd. Ook routing, DNS, kernprotocollen en technische standaarden worden hierin betrokken. Wat is de reactie van het kabinet hierop en is het kabinet het eens met de definitie van de publieke kern van het internet zoals deze wordt gebruikt in het WRR-advies?

VII. Antwoord van het Kabinet:
Het kabinet neemt als uitgangspunt dat de kernprotocollen van het internet de publieke kern vormen. Hieronder vallen in ieder geval het Transmission Control Protocol (TCP) en het internetpro-

tocol (IP), samen TCP/IP, onderdeel van de zogenoemde internet protocol suite. De definitie van de WRR is niet conclusief en ook internationaal is er nog geen overeenstemming over wat precies nog meer onder de definitie van de publieke kern valt. Het kabinet moedigt daarom verder onderzoek naar en discussie over gedragsnormen voor de bescherming van of zelfs non-interventie op (onderdelen van) de publieke kern van het internet aan. Hierbij zal er dieper worden ingegaan op wat de publieke kern van het internet omvat. In die overwegingen zullen ook Domain Name System (DNS) en andere mogelijke protocollen en standaarden, zoals die voor routing, worden meegenomen.

Het kabinet stelt zich op het standpunt dat de aard en de afhankelijkheid van het digitale domein vragen om terughoudendheid ten aanzien van activiteiten die aan de publieke kern kunnen raken en neemt dit dus ook als uitgangspunt wanneer overheidshalve inbreuk op de technische werking van het internet aan de orde kan zijn. Hierbij zal altijd een balans moeten worden gevonden tussen vrijheid, veiligheid en economische belangen. Wanneer het noodzakelijk is om aan de technische werking van het internet te raken, zal altijd worden getoetst aan bestaand nationaal en internationaal recht.

Dan lezen de leden van de PvdA-fractie dat het kabinet stelt dat de aanpak van cybersecurity en het waarborgen van de nationale veiligheid vraagt om een geïntegreerde benadering. De leden van de PvdA-fractie vragen zich af waaruit deze geïntegreerde benadering op dit moment blijkt. Volgens de leden van de PvdA-fractie lijkt het er momenteel op dat elk van de afzonderlijke departementen bezig is met het ontwikkelen van eigen beleid voor informatieveiligheid. Op welke wijze wordt er op dit moment tussen de verschillende departementen afgestemd of het waarborgen van de kernwaarden van het internet of het waarborgen van veiligheid zwaarder weegt en of inbreuken op de publieke kern van het internet geoorloofd zijn?

VIII. Antwoord van het Kabinet:
Zie antwoord IV op de vragen van de leden van de VVD-fractie.

Ook lezen de leden van de PvdA fractie dat het kabinet de rol van de Internet Engineering Task Force (IETF) en technische gemeenschap wil behouden en versterken. Hoe zal dit worden vormgegeven? Zo staat bijvoorbeeld het instituut SURFsara, de kweekvijver van mensen die in het vormgeven van internationale governance van het internet een essentiële rol hebben gespeeld en spelen, voortdurend ter discussie. Betekent dit dat het kabinet een rol zal gaan spelen in de financiering van SURFsara? Hoe ziet het kabinet haar rol hier precies? De leden van de PvdA-fractie lezen tevens dat het kabinet zal onderzoeken of het mogelijk is groepen met een belangrijke rol voor het onderhoud van het technische niveau van de publieke kern van het internet beter te ondersteunen. Betekent dit dat het kabinet de open-source community financieel zal gaan ondersteunen? Hoe zal deze ondersteuning verder vorm krijgen? Het initiatief van het Kamerlid Oosenbrug voor een Open Source expertisecentrum zou hier een belangrijk onderdeel van kunnen zijn. Kan het kabinet hier op in gaan?

IX. Antwoord van het Kabinet:
Het kabinet beschouwt IETF als een van de belangrijkste gremia voor het ontwikkelen en verspreiden van internetstandaarden en ziet haar als complementair aan andere standaardisatie-organisaties, zoals de Internet Telecom Union (ITU) en World Wide Web Consortium (W3C). Het kabinet continueert het stimuleren

van door IETF bepaalde internetstandaarden, via het Platform Internetstandaarden en de website internet.nl.

De technische gemeenschap wordt expliciet en consequent betrokken bij de standpuntbepaling door de overheid over kwesties die het internet betreffen, neemt deel aan internationale samenwerkingsverbanden als het Global Forum on Cyber Expertise (GFCE). De technische gemeenschap heeft daarnaast een eigenstandige rol in organisaties als IETF, Internet Corporation for Assigned Names and Numbers (ICANN) en Réseaux IP Européens (RIPE). Momenteel is er geen sprake van ondersteuning van deze organisaties, of van een onderzoek naar de wenselijkheid daarvan. Wel ondersteunt het kabinet projecten als open source encryptie met € 500.000,– (Kamerstuk 34 300 XIII, nr. 171).

De overheid heeft geen directe financiële band met SURFsara, maar met de holding SURF waar SURFsara deel van uitmaakt. OCW stelt sinds 2014 structureel € 18,5 mln aan SURF ter beschikking en aanvullend € 6 mln voor 2016–2019. EZ heeft aanvullend € 19 mln ter beschikking gesteld voor 2011–2019.

Binnen de regeling Toekomstfondskrediet voor Onderzoeksfaciliteiten (TOF-regeling) is nog eens € 11,1 mln geoormerkt voor investeringsvoorstellen voor de ICT-infrastructuur van het wetenschappelijk onderzoek en onderwijs, zoals uitgevoerd door het samenwerkingsverband SURF (Kamerstuk 34 300 VIII, Nr. 543).

Ten slotte wordt in de kabinetsreactie gesproken over de dialoog met het bedrijfsleven. Uit het WRR-rapport blijkt echter dat er een onderscheid kan worden gemaakt tussen activiteiten van bedrijven die betrekking hebben op de publieke kern van het internet en privacy, veiligheid en vrijheid in het digitale domein beschermen, en bedrijven die door hun wereldwijde dominante marktpositie negatieve invloed hebben op de publieke kern van het internet. Het kabinet stelt dat deze laatste categorie bedrijven «serieuze diplomatieke aandacht verdienen». Het kabinet spreekt vervolgens van een dialoog en samenwerking met deze bedrijven. De leden van de PvdA-fractie vinden dit weinig concreet. Hoe zorgt het kabinet ervoor dat die dialoog en samenwerking leidt tot de bescherming van de publieke kern van het internet? Hoe gaat het kabinet de dialoog en samenwerking met bedrijven uitbreiden en coalities sluiten met nieuwe internetbedrijven en ngo's?

X. Antwoord van het Kabinet:
De dialoog met het bedrijfsleven vindt continu plaats en kent vele vormen, van beleidsvoorbereiding, onder meer voor de visie Telecom, internet en media (2015) en de visie Frequentiebeleid (2016), tot consultaties van wet- en regelgeving en overleg over de standpunten in internationale gremia als Internet Corporation for Assigned Names and Numbers (ICANN) en International Telecommunication Union (ITU). De publieke belangen die aanleiding vormen voor beleidsmaatregelen worden daarbij over en weer verhelderd, waaronder maatregelen die kunnen bijdragen aan de bescherming van de publieke kern en maatregelen die daar om zwaarwegende redenen vanaf zouden kunnen wijken. Over veiligheidsvraagstukken in het digitale domein overleggen private en publieke partners onder andere in de Cyber Security Raad.

Inbreng van de leden van de fractie van D66

De leden van de D66-fractie hebben kennis genomen van de kabinetsreactie op het AIV-advies «Het internet, een wereldwijde vrije ruimte met begrensde staatsmacht» en het WRR advies «De publieke kern van het internet: naar een buitenlandse internetbeleid». De leden danken beide adviesorganen voor hun advies en onderschrijven het belang van hun bevindingen. De leden hebben echter wel nog vragen en opmerkingen naar aanleiding van de reactie van het kabinet.

De leden van de D66-fractie constateren dat het kabinet geen eenduidige reactie op de gegeven adviezen geeft. Het kabinet zegt dat het de analyse van de AIV en WRR als aansporing ziet om zijn huidige internetbeleid te versterken. Het kabinet geeft echter ook aan dat het nog een internationaal cyberbeleid moet gaan formuleren. De genoemde leden vragen zich af hoe de adviezen als een bemoediging van het huidige beleid kunnen worden gezien als dit beleid nog niet eens is vastgesteld? Wanneer kan de Kamer de visie van het kabinet verwachten? De betreffende leden constateren dat het kabinet, ondanks de verwevenheid van de uitdagingen op internet-gebied, de beleidsverantwoordelijkheid van ministeries niet wil aantasten. Wie zal er eindverantwoordelijkheid dragen voor de formulering en de implementatie van de strategie?

XI. Antwoord van het Kabinet:
De kabinetsreactie geeft aan dat om maximaal te kunnen blijven profiteren van de kansen die het internet biedt een robuuste nationale en internationale cyberstrategie nodig is. De aangekondigde internationale strategie zal complementair zijn aan en in lijn zijn met nationale beleidskeuzes op het gebied van cyber. Het kabinet benadrukt het belang van consistentie tussen binnenlands en buitenlands beleid om effectief in te kunnen zetten op een vrij, open en veilig internet. Een internationale cyberstrategie geeft hieraan invulling.

Omdat cyber een beleidsterrein is dat raakt aan verschillende departementen, zal de internationale strategie een breed gedragen strategie worden waar de relevante departementen gezamenlijk voor verantwoordelijk zijn. Daarnaast zal het kabinet veelvuldig en op zorgvuldige wijze consulteren met het maatschappelijk middenveld, de technische gemeenschap en de private sector. De internationale strategie zal daarom in het voorjaar van 2017 aan de Tweede Kamer kunnen worden toegezonden.

De leden van de D66-fractie constateren met tevredenheid dat het kabinet het belang van een «publieke kern» van het internet beschouwt als een voorwaarde voor het goed functioneren van het internet. Kan het kabinet aangeven waarom het niet net als het WRR-rapport zaken als routing, DNS, kernprotocollen en technische standaarden heeft meegenomen in de definitie van de «publieke kern» van het internet? Is het kabinet bereid zijn definitie te verbreden zodat deze ook de genoemde zaken omvat? Zo nee, waarom niet? Kan het kabinet toelichten hoe zijn internationale cyberbeleid zaken als routing, DNS, kernprotocollen en technische standaarden wil waarborgen? Kan het kabinet toezeggen dat het in het nog te formuleren beleid de waarborging van internet als mondiaal publiek goed tot een speerpunt maakt? Zo nee, waarom niet? Kan het kabinet toezeggen dat het voorstellen waarin overheidshalve inbreuk wordt gemaakt op de technische werking van het internet, niet zal steunen?

XII. Antwoord van het Kabinet:
Zie antwoord VII op de vragen van de leden van de PvdA-fractie.
Hoe draagt het kabinet bij aan het wijder gebruik van nieuwe technologieën en standaarden die bijdragen aan de veiligere werking van het internet, zoals DNSSEC of IPv6? Kan het kabinet garanderen dat alle websites van de Nederlandse overheid voldoen aan alle deze protocollen en standaarden? Zo niet, wanneer zal dit wil het geval zijn?

XIII. Antwoord van het Kabinet:
Voor deze standaarden is door het Nationaal Beraad een adoptie-impuls afgesproken. Het streven is om de beveiligingsstandaarden, die reeds op de pas-toe-of-leg-uit-lijst staan, uiterlijk eind 2017 te hebben geïmplementeerd waar dat van toepassing is. Het Forum Standaardisatie meet op verzoek van het Nationaal Beraad halfjaarlijks de voortgang van de adoptie van deze standaarden door een aantal veelgebruikte domeinnamen van de partijen in het Nationaal Beraad. De gebruikscijfers van o.a. DNSSEC (domeinnaam beveiliging) laten in 2014 en 2015 een flinke groei zien, van respectievelijk 18 en 15 procent.

Internet Protocol versie 6 (IPv6) maakt geen deel uit van de bovengenoemde adoptie-impuls maar staat wel al jaren op de pas-toe-of-leg-uit-lijst (evenals DNSSEC). Standaarden die op deze lijst staan moeten verplicht gebruikt worden bij aanschaf, aankoop, ontwikkeling of aanbesteding van nieuwe diensten, tenzij er een zwaarwegende reden is om hiervan af te wijken. Hoe snel IPv6 geïmplementeerd wordt is daardoor afhankelijk van het tempo waarin de overheid ICT-systemen vervangt of bijwerkt. Desalniettemin wordt de implementatie van IPv6 bij de overheid op twee manieren gestimuleerd. Ten eerste doordat het IPv6-adresblok dat voor de rijksoverheid was aangeschaft in 2016 uitgebreid is met een tweede adresblok dat gebruikt kan worden door provincies, waterschappen en gemeenten, waardoor ook zij vanuit dit gezamenlijke kader IPv6 kunnen implementeren. Ten tweede is IPv4 onderhand nog maar zeer beperkt beschikbaar zodat in de nabije toekomst uitsluitend IPv6 nummers zullen worden uitgegeven.

Om de implementatie van IPv6 door de markt te stimuleren heeft het Ministerie van Economische Zaken de Task Force IPv6 financieel ondersteund tot 2016. De beschikbare middelen in 2016 om IPv6 te stimuleren zijn opgegaan in het Platform Internetstandaarden, dat de test tool www.internet.nl heeft ontwikkeld. Daarmee is de subsidie voor de IPv6 taskforce beëindigd maar is er vanaf 2016 een financiële bijdrage aan het platform. De taskforce blijft doorgaan als expertgroep en -netwerk, en werkt nauw samen met het nieuwe Platform Internetstandaarden. Het platform en de taskforce zijn marktbreed.

De leden van de D66-fractie constateren dat het kabinet uitvoering gaat geven aan de motie van D66 om te onderzoeken of Nederland groepen in de technische wereld, zoals ontwikkelaars van open source encryptie, die bijdragen aan het goed functioneren van het internet, financieel kan steunen. Kan het kabinet aangeven welke vragen het met dit onderzoek wil beantwoorden en op welke termijn het onderzoek zal worden uitgevoerd?

XIV. Antwoord van het Kabinet:
Zie antwoord IV op vragen van de leden van de VVD-fractie.

De leden van de D66-fractie constateren dat het kabinet de aanbeveling van de WRR overneemt om het principe van «practice what you preach» centraal te laten staan in het internationale internetbeleid. Dit verbaast hen, aangezien het kabinet onlangs het wetvoorstel op de kansspelen naar de Kamer heeft gestuurd, waarin een bevoegdheid voor de Kansspel Autoriteit gecreëerd wordt waarmee de overheid ingrijpt op de technische werking van het internet In hoeverre onderstreept het kabinet de aanbeveling van de WRR om niet in te grijpen op de technische werking van het internet en hoe verhoudt zich dit tot het wetsvoorstel op de kansspelen?

XV. Antwoord van het Kabinet:
Nederland erkent dat de aard en de afhankelijkheid van het digitale domein vragen om terughoudendheid ten aanzien van activiteiten die aan de publieke kern kunnen raken. Daarnaast zet het kabinet er zich voor in dat de instandhouding en ontwikkeling van de «publieke kern» zoveel mogelijk blijft voorbehouden aan de technische gemeenschap en de statelijke rol zich zo veel mogelijk richt op de ondersteuning daarvan. De wet kansspelen op afstand grijpt, geheel in lijn met bovengenoemd standpunt, niet in op de technische werking van het internet.

De leden van de D66-fractie constateren dat de AIV de aanbeveling doet om het onafhankelijk toezicht op de inlichtingen- en veiligheidsdiensten, alsmede het toezicht door het College Bescherming Persoonsgegevens te versterken. Is het kabinet bereid deze aanbeveling over te nemen? Zo nee, waarom niet?

XVI. Antwoord van het Kabinet:
Het kabinet hecht aan effectief en onafhankelijk toezicht. Per 1 januari 2016 zijn de bevoegdheden van de Autoriteit Persoonsgegevens (AP) voor het uitoefenen van haar handhavende taken verstevigd door de invoering van de uitbreiding boetebevoegdheid en de meldplicht datalekken. Daarnaast heeft het inzicht dat de huidige stand van de techniek om een sterk regelgevend kader vraagt, geleid tot het aannemen van de Algemene verordening gegevensbescherming en de richtlijn. Hiermee wordt onder andere voorzien in een versterking van de bevoegdheden en middelen die de AP tot haar beschikking heeft.

De leden van de D66-fractie constateren dat het kabinet de gidsrol van Nederland op het gebied van mondiale internetvrijheid wil koesteren. Welke effecten zal het voornemen van het kabinet om Nederlandse veiligheidsdiensten in staat te stellen om zonder rechtshulpverzoek computers in het buitenland te mogen hacken of het voorstel om sleepnettechnieken toe te passen op de data die door Nederland gaan, hebben op de bereidheid van andere landen om Nederland als gidsland te beschouwen? Hoe rijmt het kabinet deze wetsvoorstellen met het idee van «practice what you preach»? En kan het kabinet garanderen aan internetgebruikers, waar dan ook ter wereld, dat hun data in Nederland veilig en vertrouwelijk zijn en blijven?

XVII. Antwoord van het Kabinet:
De bevoegdheid tot binnendringen in geautomatiseerd werk ten behoeve van opsporing van strafbare feiten wordt geregeld in het wetsvoorstel Computer Criminaliteit III. De uitvoering hiervan is weergegeven in de memorie van toelichting van dat wetsvoorstel. De bevoegdheid tot binnendringen in geautomatiseerd werk van de inlichtingendiensten wordt geregeld in de Wet op de inlichtingen- en veiligheidsdiensten. Een nieuwe wet op de

inlichtingen- en veiligheidsdiensten is voorbereid ter vervanging van de huidige wet uit 2002. Het wetsvoorstel is thans voor advies aanhangig bij de Afdeling Advisering van de Raad van State. In het wetsvoorstel wordt het toezicht op de inlichtingen- en veiligheidsdiensten in meerdere opzichten versterkt. Zo voorziet het voorstel bij de inzet van de meest inbreukmakende bevoegdheden in een voorafgaande, bindende toets door een onafhankelijke commissie van leden met een rechterlijke achtergrond. Tevens wordt de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) gepositioneerd als een zelfstandige, onafhankelijke klachtinstantie die naar aanleiding van klachten bindende oordelen kan gaan geven. Het kabinet streeft ernaar het wetsvoorstel zo spoedig mogelijk na ontvangst van het advies van de Raad van State toe te zenden aan de Tweede Kamer.

Zoals in de kabinetsreactie vermeld, benadrukt het kabinet het belang van consistentie tussen binnenlands en buitenlands beleid. De hierboven benoemde wetsvoorstellen vormen hierop geen uitzondering. Enerzijds dienen de internationale standpunten van Nederland te volgen uit de nationale praktijk en is «preach what you practice» een uitgangspunt. Anderzijds leiden voorgenomen nationale maatregelen die afwijken van internationaal in te nemen standpunten en internationale verdragsverplichtingen tot een vermindering van geloofwaardigheid en effectiviteit bij het streven naar internationale ordening. In dat opzicht geldt ook «practice what you preach» als een uitgangspunt van nationaal beleid. Uiteraard geldt dat Nederland pas gehouden is aan internationale regelgeving als daarover internationaal overeenstemming is bereikt en Nederland de betreffende verplichting is aangegaan.

Het kabinet geeft aan het Europese Voorzitterschap van Nederland te willen benutten om op Europees niveau de wet- en regelgeving aangaande internetvrijheid te moderniseren. Welke concrete successen heeft het kabinet hierbij behaald?

XVIII. Antwoord van het Kabinet:
Zie antwoord VI op vragen van de PvdA-fractie.

Op het mondiale toneel zegt het kabinet zich te richten op het beïnvloeden van zogenaamde *«swing states»* op het gebied van internetvrijheid. Kan het kabinet aangeven welke staten het hierbij in gedachten heeft en hoe het deze wil aanpakken? Wat betekent dit voor de inspanningen die het kabinet gaat plegen richting landen die repressief optreden op het gebied van internetvrijheid? Hoe blijft Nederland landen waar de digitale mensenrechten structureel geschonden worden, attenderen op het belang van internetvrijheid? Welke prioriteit gaat het kabinet dit onderwerp geven in de bilaterale contacten met deze landen?

XIX. Antwoord van het Kabinet:
Het kabinet ziet het belang om bepaalde landen die nog niet hebben gekozen voor het respecteren van de integriteit van het internet ervan, te overtuigen dat zij vanuit hun nationale belangen ook baat hebben bij een open, vrij en veilig internet. Om het meeste effect te sorteren, worden op dit moment meerdere instrumenten in onderlinge afstemming ingezet. Daarnaast biedt NL zijn expertise en kennis aan, aan die staten die baat hebben bij opbouw van capaciteit voor beleids- of strategievorming. Hieraan wordt momenteel al gewerkt met het Global Forum on

Cyber Expertise (GFCE). Het kabinet is er voorts van overtuigd dat betrokkenheid van alle relevante stakeholders een voorwaarde is voor de totstandkoming van een vrij, open en veilig internet. Derhalve wordt in onder andere Kenia en Indonesië gewerkt aan het stimuleren van een multistakeholderdialoog op het gebied van cybersecurity.

Concreet werkt Nederland in een aantal gremia aan internetvrijheid. Zo biedt de Freedom Online Coalitie mogelijkheden voor zowel samenwerking met «swing states», als om online schendingen van mensenrechten aan te kaarten. Dit gebeurt o.a. door gezamenlijk verklaringen op te stellen over onacceptabel optreden van staten, publiekelijk en achter de schermen. Daarnaast bieden bilaterale contacten en de mensenrechten- en cyberdialogen tussen de EU en derde landen de kans om ontwikkelingen die een open, vrij en veilig internet stimuleren te benoemen en te prijzen maar tevens online schendingen van mensenrechten af te keuren. In VN-verband zet Nederland zich actief in voor vooruitstrevende resoluties over mensenrechten online. Tenslotte steunt Nederland projecten die erop gericht zijn om mensenrechtenverdedigers en activisten te helpen hun werk voort te zetten in een omgeving waar hun vrijheid niet vanzelfsprekend is.

De leden van de D66-fractie constateren met tevredenheid dat het kabinet uitvoering geeft aan de motie van het lid Verhoeven om de Nederlandse internetinfrastructuur tot derde mainport uit te roepen. Ook zijn de betreffende leden blij met de bereidheid van het kabinet om ruimte te bieden aan ethische hackers door »*responsible disclosure*« mogelijk te maken. De Nederlandse digitale infrastructuur behoort tot de beste ter wereld. Dit creëert een aantrekkelijk vestigingsklimaat en biedt geweldige economische kansen voor individuen en bedrijven. De betreffende leden roepen het kabinet op om dit ook internationaal nadrukkelijk uit te dragen.