Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 475

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 23 juni 2017

De vaste commissie voor Buitenlandse Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Buitenlandse Zaken over de brief van 12 februari 2017 over de Internationale Cyberstrategie (Kamerstuk 26 643, nr. 447).

De vragen en opmerkingen zijn op 6 april 2017 aan de Minister van Buitenlandse Zaken voorgelegd. Bij brief van 1 juni 2017 zijn de vragen beantwoord.

De fungerend voorzitter van de commissie,
Omtzigt

De griffier van de commissie,
Van Toor

kst-26643-475
ISSN 0921 - 7371
's-Gravenhage 2017

Vragen en opmerkingen vanuit de fracties en reactie van de Minister van Buitenlandse Zaken

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? 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?

1. Antwoord van het kabinet:
De strategische nationale veiligheidsbelangen kunnen niet worden bewaakt zonder het helpen van andere landen met capaciteitsopbouw op het gebied van cybersecurity. Capaciteitsopbouw op het terrein van cybersecurity is dan ook noodzakelijk. Op de korte termijn helpt capaciteitsopbouw bij het verbeteren van de digitale weerbaarheid van partnerlanden en voorkomt het dat cyberdreigingen ontstaan die ook in Nederland schade kunnen berokkenen. Op de lange termijn helpen investeringen van Nederland in capaciteitsopbouw om strategische allianties op te bouwen gericht op het ondersteunen van een vrij, open en veilig internet en aanverwante Nederlandse beleidsdoelstellingen.

In het Global Forum on Cyber Expertise (GFCE) dat tijdens de Global Conference on Cyber Space (GCCS) in 2015 door Nederland is gelanceerd, worden initiatieven voor het delen van kennis en kunde over digitale veiligheid samengebracht. Op dit moment zijn 36 landen lid van het GFCE. Binnen het GFCE heeft Nederland als co-voorzitter een sturende en zichtbare rol. Vanuit die rol is Nederland vijf initiatieven gestart op de volgende terreinen: i) versterken van Computer Security Incident Response Teams (CSIRTs), ii) aanmoedigen van het implementeren van veilige internetstandaarden, iii) het verhogen van de Critical Information Infrastructure Protection iv) het stimuleren van Coordinated Vulnerability Disclosure en v) een regionaal initiatief in (West) Afrika over bewustwording op het terrein van cybersecurity.
Nederland heeft diverse expertbijeenkomsten voor GFCE leden op deze thema's georganiseerd. Dit heeft ertoe geleid dat good practices van Nederland op deze thema's worden onderschreven en internationaal verder worden uitgedragen, onder andere tijdens de GCCS eind 2017 in India. Vervolgens moet dit resulteren in capaciteitsopbouwinitiatieven op hierboven weergegeven terreinen.

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?

2. Antwoord van het kabinet:
Nederland draagt bij aan het vergroten van de betrokkenheid van ontwikkelingslanden bij het mondiale IGF via jaarlijkse donaties aan het door de VN beheerde IGF Trust Fund.[1] Uit dit multi-donorfonds subsidieert het IGF-secretariaat workshops in ontwikkelingslanden over capaciteitsopbouw alsook deelname van ontwikkelingslanden aan een fellowshipprogramma van het IGF-secretariaat om ervaring op te doen in het beleidsdebat over internet governance.

Via het IGF discussiëren diverse stakeholdergroepen over uiteenlopende internetvraagstukken en delen kennis en praktijkervaring die waar mogelijk worden vastgelegd in «best practices» documenten. Nederland is via het Nederlands Internet Governance Forum (NLIGF) actief daarbij betrokken. Een tastbaar resultaat van het IGF is het handboek over de «Best Practices Forums» van 2015. Daarin staan aanbevelingen van deze werkgroepen van het IGF met «best practices» voor onder meer het opzetten van internetknooppunten, het toepassen van veilige internetstandaarden, het bieden van ondersteuning bij en afhandelen van cybersecurity incidenten (CSIRTs) en spambestrijding. Sinds 2016 is Nederland overheidslid van de multistakeholder adviesgroep van het IGF die de Secretaris-Generaal van de VN adviseert over de agenda van de jaarlijkse IGF-bijeenkomsten. Ook daar maakt Nederland zich hard voor een inclusief, zichtbaar en financieel stabiel IGF, met verkleining van de digitale kloof als één van de prioriteiten.

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?

3. Antwoord van het kabinet:
De Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIB-richtlijn), die voortvloeit uit de Europese cyberstrategie, richt zich op de beveiliging van netwerk- en informatiesystemen van aanbieders van essentiële diensten en digitale-dienstverleners. Hierover is de Kamer via de voortgangsbrieven van 3 december 2015 (Kamerstuk 33 602, nr. 7) en 24 juni 2016 (Kamerstuk 33 602, nr. 8) geïnformeerd.

Lidstaten hebben de vrijheid om binnen de in bijlage II van de richtlijn genoemde sectoren, aan de hand van in de richtlijn vermelde criteria, zelf te bepalen welke specifieke aanbieders onder de bepalingen van de richtlijn komen te vallen. Bij de Nederlandse aanwijzing van de aanbieders van essentiële diensten zal de lijst van Nederlandse vitale processen, zoals opgenomen in de voortgangsbrief Nationale Veiligheid van 2015 (Kamerstuk 30 821, nr. 23) en de voortgangsbrief Nationale Veiligheid 2016 (Kamerstuk 30 821, nr. 32) nadrukkelijk als uitgangspunt dienen. De implementatie van de NIB-richtlijn in nationale wetgeving is thans gaande. Het wetsvoorstel zal naar

[1] **Nederland is één van de belangrijkste financiële donoren van het IGF. De Nederlandse financiële bijdrage aan het IGF Trust Fund bedroeg over de periode 2006–2010 $ 194.827,50 en over de periode 2011–2016 $ 154.610.**

verwachting in het najaar van dit jaar in procedure worden gebracht.

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?

4. Antwoord van het kabinet:
Het IGCI is opgezet in april 2015 om internationale samenwerking tussen politiediensten te realiseren, zo mogelijk in nauwe samenwerking met de private sector en met een accent op cybercrime. Op dit moment wordt nauw samengewerkt met de antivirus-industrie en het bankwezen. IGCI ondersteunt in de coördinatie van de wereldwijde opbouw van cybercapaciteit. Daarnaast is IGCI de plek waar kruisverbanden gelegd kunnen worden tussen gegevens uit diverse jurisdicties. Ten slotte biedt IGCI aan cyberrecherche wereldwijd de kans om kennis te bundelen, bijvoorbeeld door INTERPOL te laten aansluiten op het Nederlandse initiatief NoMoreRansom.org en aldus te streven naar aansluiting van de 190 INTERPOL-staten, een gedeelde stem te laten horen in internationale gremia, zoals Internet Corporation for Assigned Names and Numbers (ICANN), de International Standardization Organization (ISO), de International Telecommunication Union (ITU), het World Economic Forum en om specifieke trainingen aan te bieden om alle spelers binnen de internationale opsporingsketen op hetzelfde vereiste (basis-)niveau te krijgen. Zo wordt er expertise opgebouwd op het gebied van «dark markets» en «virtual currencies» door onder meer het wereldwijd uitrollen van een recherchetraining in samenwerking met TNO. Inmiddels is ook de Koninklijke Marechaussee aangesloten op het INTERPOL-cybernetwerk.

Concrete resultaten in de operationele ondersteuning zijn tot dusverre dat er enkele honderden waarschuwingsberichten over cybercriminaliteit zijn uitgegaan, dat er intercontinentale coördinatie heeft plaatsgehad ten aanzien van de ontmanteling van criminele netwerken en infrastructuren waaronder vijf botnets (softwarerobots die automatisch spam verspreiden) zoals het Simda-botnet, en sextortion-bendes, dat er technisch-forensische ondersteuning is geboden (deblokkeren van mobiele telefoons van (onder meer Nederlandse) verdachten en onderzoeken van geavanceerde digitale bankroven en beveiligingsmaatregelen), dat er informatie is uitgewisseld in internationale cyberfraude-onderzoeken (identificeren van daders en (onder meer Nederlandse) slachtoffers van CEO-fraude (waarbij criminelen zich digitaal voordoen als CEO van het bedrijf) en internationale webshopfraude tegen (onder meer) Nederlandse slachtoffers) en dat criminele programmatuur en netwerk van dienstverleners zijn geanalyseerd (zoals «keyloggers», waarmee (ook Nederlandse) verdachten identiteiten hebben gestolen en onderzoeken malware en signaleren van gerelateerde (ook Nederlandse) dienstverleners).
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?

5. Antwoord van het kabinet:
Op 16 september 2016 heeft de Cloud Evidence Group, een subgroep van het comité van verdragspartijen van het Cybercrimeverdrag uit 2001, zijn eindrapport uitgebracht. Het eindrapport bevat diverse aanbevelingen voor het versterken van de mogelijkheden voor toegang tot digitaal bewijs in de cloud ten behoeve van strafrechtelijke handhaving. Eén van de aanbevelingen betreft het voorbereiden van een concept voor een additioneel protocol bij het verdrag. Tijdens de bijeenkomst van het comité van verdragspartijen op 14 en 15 november 2016 heeft het comité bij consensus besloten dat er in beginsel een noodzaak is voor een additioneel protocol. Ten behoeve van een formeel besluit van het comité om een conceptprotocol op te stellen, is de Cloud Evidence Group verzocht Terms of Reference voor een dergelijk proces uit te werken. Deze Terms of Reference worden in juni verwacht. Op het verdere verloop van de discussie kan niet vooruit gelopen worden.

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.

6. Antwoord van het kabinet:
De NAVO-lidstaten zijn het erover eens dat het bondgenootschap sterker staat wanneer de lidstaten hun eigen zaken op orde hebben. Daarom is door alle lidstaten de belofte uitgesproken dat de inspanningen op het gebied van cybersecurity blijvend worden verhoogd. Daarmee heeft ook Nederland uitgesproken aandacht te blijven besteden aan cybersecurity. Er zijn voor Nederland geen specifieke verplichtingen verbonden aan de Cyber Defence Pledge.

Nederland is al enige tijd bezig met het versterken van de cybersecurity. Met de Nationale Cyber Security Strategie (NCSS) 2 (Kamerstuk 26 643, nr. 291) is het beleid er reeds op gericht om onze digitale weerbaarheid te verhogen. Dit doen we bijvoorbeeld door te investeren in het vroegtijdig detecteren van aanvallen, de aanpak van cybercrime, de opbouw van militaire capaciteiten in het cyberdomein en het versterken van het diplomatiek instrumentarium.

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?

7. Antwoord van het kabinet:
De schade voor de economie als gevolg van digitale onveiligheid laat zich lastig eenduidig kwantificeren (Centraal Planbureau, Risicorapportage Cyberveiligheid Economie, 2016). Rapporten die ingaan op de economische schade van cybercriminaliteit, zijn doorgaans gebaseerd op schattingen van experts, of enquêteresultaten die worden geëxtrapoleerd en al dan niet geprojecteerd op andere landen. De schattingen lopen sterk uiteen, zoals eerder aangegeven in de antwoorden op vragen van het lid Recourt (PvdA) van 13 juni 2014 (Aanhangsel Handelingen II 2013/14, nr. 2703).

Er zijn al met al voor de komende jaren geen reële prognoses te geven van de toe- of afname van schadebedragen ten gevolge van cybercrime en cyberspionage. Voor de wijze waarop de dreiging zich ontwikkelt wordt verwezen naar het Cyber Security Beeld Nederland (CSBN) dat jaarlijks door het Ministerie van Veiligheid en Justitie aan de Kamer wordt aangeboden.

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?

8. Antwoord van het kabinet:
Zie antwoord 37 op vragen van de leden van de SP-fractie.

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?

9. Antwoord van het kabinet:
Het kabinet onderkent het toenemende belang van defensieve en offensieve slagkracht in het cyberdomein. Daarom is in 2012 besloten om het Defensie Cyber Commando (DCC) op te richten, zodat deze slagkracht bij de krijgsmacht kan worden opgebouwd. Sindsdien is het DCC in 2015 formeel opgericht en is datzelfde jaar besloten om extra geld te investeren in cybercapaciteiten bij defensie (Kamerstuk 34 000, nr. 1).
Zoals ook bij andere onderwerpen het geval is, heeft het kabinet hierbij aandacht voor de balans tussen beschikbare middelen, capaciteiten en taken. Daarnaast heeft Defensie in het meerjarig perspectief de ambitie uitgesproken om in de toekomst te blijven investeren in de defensieve en offensieve slagkracht in het cyberdomein (Kamerstuk 33 763, nr. 126).

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?

10. Antwoord van het kabinet:
Gezien het toenemend belang van het internationale cyberdomein is het van essentieel belang dat de Nederlandse diplomatie ook op dit terrein onze nationale belangen behartigt. De regering heeft het postennet daartoe specifiek geïnstrueerd. Het netwerk heeft reeds goed geanticipeerd op een aantal dreigingen en kansen, bijvoorbeeld in het kader van de Global Conference on Cyber Space (GCCS) in 2015 te Den Haag. Tegen de achtergrond van de in de Internationale Cyberstrategie (ICS) (Kamerstuk 26 643, nr. 447) geschetste kansen en uitdagingen alsook toenemende dreigingen van onder meer kwaadwillende statelijke actoren, is versterking van deze inzet noodzakelijk.

Het is daarbij van belang dat cyberdiplomaten kunnen bouwen op solide cyberkennis, diplomatieke ervaring, kennis en vaardigheden. Bij de verdere uitbouw van het diplomatennetwerk wordt ook gekeken naar de ervaringen en best practices van andere landen, zoals onder meer het VK en de VS, die een soortgelijke aanpak hanteren. Het kabinet zal de Tweede Kamer informeren over voortgang met betrekking tot de ICS.

Het takenpakket van een cyberdiplomaat ziet er grosso modo als volgt uit:
- **liaison voor samenwerking op het internationale cyberbeleid.**
- **knooppunt voor kennis en analyse over trends en ontwikkelingen in het cyberdomein in den brede.**
- **management van samenwerkingsprogramma's en projecten daar waar relevant.**

Teneinde de kennis van cyberdiplomaten te versterken worden trainingsprogramma's, terugkom- en netwerkdagen georganiseerd. Het netwerk wordt vooralsnog binnen de bestaande formatie bij wijze van pilot onder meer op de posten Washington, Londen, Beijing en Moskou geactiveerd. Een nieuw kabinet kan de internationale benadering van het cyberdomein versterken door ook andere belangrijke landen binnen en buiten Europa in aanmerking te laten komen om deel uit te maken van het cyberdiplomatennetwerk en middelen ter beschikking te stellen.

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?

11. Antwoord van het kabinet:
Gegeven de dreigingen zoals die zijn genoemd in het door het Nationaal Cyber Security Centrum (NCSC) opgestelde Cyber Security Beeld Nederland (CSBN) en het AIVD jaarverslag, is het Ministerie van Buitenlandse Zaken een doelwit voor cybercriminelen en cyberspionage. De Nederlandse ambassades zijn als onderdeel van het ministerie daarmee eveneens doelwit. Toenemende mogelijkheden van digitale technologie maken dat er sprake is van een voortdurende wedloop. De inzet blijft om met

de beschikbare capaciteit maximale weerbaarheid te realiseren om zo effectief mogelijk om te kunnen gaan met digitale aanvallen. Dit gebeurt door het verhogen van het bewustzijn rondom cybersecurity en door het nemen van adequate beveiligingsmaatregelen.

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?

12. Antwoord van het kabinet:
Het European Cyber Crime Center (EC3) heeft geen eigen politiële bevoegdheden, maar ondersteunt de EU-lidstaten in de aanpak van cybercriminaliteit. Daarbij lag de focus op cybercriminaliteit gepleegd door georganiseerde groepen, op cybercriminaliteit die ernstige schade aan hun slachtoffers toebrengt (online kinderporno) en op cybercriminaliteit die de vitale infrastructuur raakt. Daarnaast heeft EC3 EU-lidstaten ondersteund bij de aanpak van grensoverschrijdende criminaliteit (b.v. darknet gerelateerde criminaliteit, money mules, witwassen, enz.).

EC3 biedt de EU-lidstaten ondersteuning in de operationele aanpak, onder meer door coördinatie en prioritering. EC3 functioneert als een platform voor informatiedeling. Ook maakt EC3 gebruik van zijn netwerkcapaciteiten om de samenwerking met partners op het terrein van handhaving en opsporing in landen buiten de EU te bevorderen. EC3 levert op hoog niveau technische, analytische en digitale forensische expertise ter ondersteuning van onderzoeken naar cybercriminaliteit in EU-lidstaten. EC3 beschikt ook over de Europol Malware Analysis Solution (EMAS) waarmee intelligence op het terrein van schadelijke software kan worden verrijkt door onder meer analyse en forensisch onderzoek ten aanzien van de malware. Een goed voorbeeld is de bijdrage van EC3 in de aanpak van ransomware

Sinds het centrum is ingesteld, ondersteunt EC3 lidstaten bij complexe cyberonderzoeken en levert daarmee een belangrijke bijdrage aan de aanpak van complexe cybercriminaliteit. Het aantal complexe cyberonderzoeken is de afgelopen jaren gestegen: 57 in 2013, 72 in 2014, 131 in 2015 en 175 in 2016. EC3 verzamelt geen gegevens over het aantal verrichte arrestaties en het aantal opgerolde cybercriminele groepen.

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?

13. Antwoord van het kabinet:
Het mandaat van de UN Group of Governmental Experts (UN GGE) omvat naast het formuleren van aanbevelingen voor vrijwillige, niet-bindende gedragsnormen ook het bevorderen van een gemeenschappelijk begrip van de toepassing van het internationaal recht op het «gebruik van informatie- en communicatietechnologie (ICT) door Staten in de context van internationale veiligheid». In het kader daarvan hebben voorgaande bijeenkomsten van de UN GGE reeds geconstateerd dat het internationaal recht, en in het bijzonder het Handvest van de VN, van toepassing is op het gebruik van ICT door staten. Ook hebben deze groepen aandacht besteed aan hoe specifieke beginselen en regels kunnen worden toegepast in dit kader. Het primaire doel van het kabinet is dat deze UN GGE de toepasselijkheid en toepassing van een groter aantal specifieke beginselen en regels onderschrijft, zoals het recht op zelfverdediging, het humanitair oorlogsrecht en het staatsaansprakelijkheidsrecht. Overigens acht het kabinet, net als veel gelijkgestemde landen, deze beginselen en regels reeds van toepassing.

Ten aanzien van de inzet van offensieve cybercapaciteiten is het standpunt van het kabinet, dat ook in de UN GGE wordt uitgedragen, dat het internationaal recht daar op dezelfde wijze op van toepassing is als op conventionele capaciteiten, en dat het gebruik daarvan dus in bepaalde omstandigheden is toegestaan. Zie over die omstandigheden het antwoord op vraag 43.

Ten aanzien van vrijwillige, niet-bindende gedragsnormen richt het kabinet zich op het verder uitwerken van de elf gedragsnormen die in 2015 overeengekomen zijn[2]. Het kabinet pleit er ook voor dat cyberoperaties die de algemene functionaliteit van de publieke kern van het internet ondermijnen als fundamentele dreiging erkend worden, zodat dit in eventuele toekomstige VN discussies over gedragsnormen kan worden meegenomen.

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.

[2] United Nations Governmental Group of Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015.

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?

14. Antwoord van het kabinet:
De visie van het kabinet dat veiligheid en vrijheid geen tegengestelde maar complementaire belangen zijn, ligt vastgelegd in onder meer de kabinetsreactie op de AIV/WRR Rapporten (Kamerstuk 26 643, nr. 411) en de Nationale Cyber Security Strategie (NCSS) 2 (Kamerstuk 26 643, nr. 291). Door middel van een geïntegreerde benadering wordt de balans tussen veiligheid, vrijheid en maatschappelijke groei in stand gehouden. Bij het opstellen van internetbeleid worden veiligheid, vrijheid en economische groei daarom in samenhang bezien.

Voorbeeld hiervan is het encryptiestandpunt van het kabinet (Kamerstuk 26 643, nr. 383). Hierin wordt ingegaan op het belang van encryptie voor de systeem- en informatiebeveiliging van de overheid en bedrijven, en voor de grondwettelijke bescherming van de persoonlijke levenssfeer en het communicatie-geheim. Daarnaast wordt het belang van opsporing van ernstige misdrijven en bescherming van de nationale veiligheid geschetst. Een ander voorbeeld is de grondwettelijke bescherming van het brief- en telecommunicatiegeheim in het wetsvoorstel tot wijziging van artikel 13 Grondwet (Kamerstuk 33 989), zoals dat onlangs door de kamer is aangenomen. Ook hierin zijn het beschermen van de vrijheid om vertrouwelijk te kunnen communiceren in het digitale domein en het in bij de wet omschreven gevallen kunnen beperken van die vrijheid ten behoeve van opsporing van misdrijven en in het belang van de nationale veiligheid verenigd.

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?

15. Antwoord van het kabinet:
Ten aanzien van de dreiging van digitale spionage door statelijke actoren verwijst het kabinet naar het jaarlijkse Cyber Security Beeld Nederland (CSBN) en de jaarverslagen van de inlichtingen- en veiligheidsdiensten. Het kabinet doet hierover verder geen uitspraken in het openbaar.

Het diplomatieke akkoord tussen de Verenigde Staten en de Volksrepubliek China had betrekking op bepaalde vormen van digitale economische spionage. Deze afspraken zijn later ook door de G20 omarmd. Het kabinet verkent thans onder meer in EU-verband mogelijkheden voor soortgelijke afspraken.

Cyberdreigingen raken aan alle drie de internationale veiligheidsbelangen zoals weergegeven in de Internationale Veiligheidsstrategie (Kamerstuk 33 694, nr. 1). Het kabinet heeft de buitenlandpolitieke inzet op dit thema daarom geïntensiveerd zoals verwoord in de Internationale Cyberstrategie (ICS) en als onderdeel van de bredere Nationale Cyber Security Strategie (NCSS) 2. Zoals het kabinet stelt in de beleidsreactie op het Cyber Security Beeld Nederland (CSBN) 2016 (Kamerstuk 26 643, nr. 420) maken de kwantitatief en kwalitatief toenemende dreiging in combinatie met een toenemende afhankelijkheid van inherent kwetsbare ICT in Nederland dat een doorontwikkeling van de Nederlandse cybersecurity noodzakelijk is. De ICS biedt daarom een verdere operationalisering en uitwerking van de Internationale Veiligheidsstrategie.

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*?

16. Antwoord van het kabinet:
In internationale discussies over het digitale domein is sprake van een scherpe tegenstelling tussen enerzijds de multistakeholder-georiënteerde landen waaronder Nederland, die pleiten voor bescherming van de integriteit van het internet, en anderzijds de meer staatsgeoriënteerde landen die pleiten voor controle en inperking van datgene dat over het internet wordt verspreid. Tussen deze uitersten van het spectrum bevindt zich een grote groep landen die op basis van hun eigen politiek-economische en sociaal-maatschappelijke belangen geen duidelijk keuze heeft gemaakt, de zogenoemde «swing states». De uitkomst van deze keuze is bepalend voor de toekomst van het internet.

Nederland bevindt zich, met veel, maar niet uitsluitend, EU-lidstaten en de VS, aan de zijde van landen die een multistakeholder benadering voorstaan. De «swing states» omvatten verreweg de grootste groep landen, waarvan een groot aantal zich bevindt in de «Global South». De groep staatsgeoriënteerde landen zijn landen die traditioneel het belang van overheidscontrole op het internet benadrukken, zoals China en Rusland. Nederland tracht in bilateraal en multilateraal verband de

zogenoemde «swing states» te overtuigen van de gemeenschappelijke belangen van een open, veilig en vrij internet.

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?

17. Antwoord van het kabinet:
Zoals weergegeven in de kabinetsreactie op AIV advies «Het internet, een wereldwijde vrije ruimte met begrensde staatsmacht» en WRR advies «De publieke kern van het internet: naar een buitenlands internetbeleid» (Kamerstuk 26 643, nr. 411), is op verschillende beleidsterreinen, waaronder cybersecurity en de digitale agenda, een coördinatiestructuur opgezet voor standpuntbepaling en besluitvorming. Hierin participeren de Ministeries van Economische Zaken, Veiligheid en Justitie, Defensie, Buitenlandse Zaken en Binnenlandse Zaken en Koninkrijksrelaties actief. Het Ministerie van Veiligheid en Justitie heeft een coördinerende rol op het gebied van cybersecurity. Daarbij kan worden verwezen naar de beantwoording van vragen van het lid Recourt d.d. 14 augustus 2014 (Aanhangsel Handelingen II 2013/14, nr. 2703).

Het kabinet onderschrijft het belang van goede interdepartementale coördinatie om te komen tot een integrale afweging van Nederlandse belangen op het gebied van internet en heeft daarom een Internationale Cyberstrategie (ICS) ontwikkeld die complementair is en in lijn met nationale beleidskeuzes op het digitale domein. Vanuit de verantwoordelijkheid van het Ministerie van Buitenlandse Zaken voor het buitenlandbeleid, heeft het Ministerie van Buitenlandse Zaken de totstandkoming van de ICS gecoördineerd. De strategie heeft de internationale ontwikkelingen in kaart gebracht en een afwegingskader geformuleerd voor de manier waarop Nederland internationaal optimaal zijn nationale doelstellingen kan realiseren. Er is een visie ontwikkeld die recht doet aan de verwevenheid van de verschillende thema's met betrekking tot het internet. Beleidsontwikkeling en -uitvoering op de verschillende deelterreinen blijft onder verantwoordelijkheid van de relevante departementen.

Het interdepartementaal overleg dat door het Ministerie van Buitenlandse Zaken bijeen is geroepen voor de ontwikkeling van de ICS zal worden voortgezet in aanloop naar de Global Conference on Cyber Space (GCCS) in India eind 2017. In dit overleg kunnen ook zaken die betrekking hebben op de ICS worden afgestemd. Daarnaast wordt afgestemd in de reguliere overlegstructuren bestaande uit het DG overleg cybersecurity en digitale

economie en het directeuren overleg cybersecurity, ondersteund door het interdepartementale overleg cybersecurity.

Een speciaal gezant wordt ingezet om Nederland te vertegenwoordigen in relevante fora, de resultaten van de GCCS uit te dragen en de prioriteiten van Nederland op internationaal cyber gebied te bevorderen. Het is inmiddels goed internationaal diplomatiek gebruik om een speciaal gezant cyber te mandateren. Deze gezant heeft toegang tot belangrijke partijen en gremia. Om de voorloperspositie van Nederland op dit terrein te behouden, is toegang tot belangrijke gremia onontbeerlijk.

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?

18. Antwoord van het kabinet:
Er heeft tot op heden geen inzet van offensieve cybercapaciteiten plaatsgevonden. De besluitvorming van het kabinet en het informeren van de Staten-Generaal over de inzet van offensieve cybercapaciteiten verloopt via de normale procedures betreffende de inzet van de krijgsmacht. Daar waar artikel 100 van toepassing is op de betreffende militaire inzet, geldt dat eveneens voor de betrokken cybereenheden. Zoals bekend spreekt artikel 100 over de inzet of het ter beschikking stellen van de krijgsmacht ter handhaving of bevordering van de internationale rechtsorde. Zie verder het antwoord op vraag 43.

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?

19. Antwoord van het kabinet:
Zie antwoord 10 op de vragen van de leden van de PVV-fractie.

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?

20. Antwoord van het kabinet:
Het kabinet vindt preventie van groot belang. In het cyberdomein is repressie als enig gebruikt middel adequaat noch doeltreffend. Een proactieve benadering en preventieve maatregelen voorkomen zowel cybercrime als het ontstaan van conflicten in het cyberdomein of escalatie daarvan. Specifiek in het cyberdomein kan de effectiviteit van preventieve maatregelen hoger zijn en de kosten lager, vergeleken met repressieve maatregelen. Preventie past ook in de door het kabinet gestimuleerde aanpak van publiek-private samenwerking, zoals weergegeven in de Nationale Cyber Security Strategie (NCSS) 2 (Kamerstuk 26 643, nr. 291).

Vanuit het perspectief van preventie wordt het bewustzijn bij burgers en bedrijven verhoogd met instrumenten als veiliginternetten.nl en Alert Online en de communicatiecampagne Veilig Zakelijk Internetten van het Nationaal Platform Criminaliteitsbeheersing. Daarnaast werken in het PPS-project «Secure Software» de Stichting Secure Software Alliance samen met het Ministerie van Economische Zaken, het Platform voor de Informatie Samenleving (ECP), kennis instellingen en diverse marktpartijen ten behoeve van een normenkader voor het ontwikkelen van aantoonbaar veilige software. Ten slotte wordt via het PPS-platform Internetstandaarden en de Veilige E-mail Coalitie van bedrijfsleven en overheid de invoering van moderne internetstandaarden gestimuleerd waarmee veilige en versleutelde emailcommunicatie en websurfen worden bewerkstelligd. Deze initiatieven worden door EZ, BZ en V&J als Nederlandse «best practices» ingebracht in diverse relevante internationale fora als het GFCE en het IGF, en gedeeld met andere EU-lidstaten.

Bijzondere vermelding verdient de EU richtlijn netwerk- en informatiebeveiliging. De richtlijn schrijft organisaties voor de risico's voor netwerk- en informatiesystemen die zij gebruiken in kaart te brengen en passende technische en organisatorische maatregelen te nemen om die risico's te beheersen. Verder vindt in Europees verband jaarlijks in oktober de EU campagne (ECSM) plaats met als doel het besef te vergroten met betrekking tot cyberdreigingen, het vergroten van cybersecurity onder burgers en het voorzien in actuele informatie door onderwijs en het delen van «good practices».

Zoals weergegeven in de Internationale Cyberstrategie (ICS) zet het kabinet verder in op een internationaal normatief kader voor de regulering van cyberoperaties tussen staten.

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.

21. Antwoord van het kabinet:
De Nederlandse politie beschikt met het Team High Tech Crime over een professionele capaciteit voor het opsporen van cybercrime. Het team richt zich vooral op nieuwe, technisch complexe en grote internationale onderzoeken. Daarnaast werkt de

nationale politie aan de opbouw van de capaciteit voor de bestrijding van cybercrime en voor de opsporing in cyberspace op regionaal niveau. In elke regionale eenheid wordt een cyberteam opgericht, waarmee niet alleen de capaciteit in de regionale eenheden wordt versterkt, maar ook capaciteit bij de Landelijke Eenheid meer kan worden gericht op de technisch complexe en grote internationale onderzoeken.

Het Openbaar Ministerie beschikt, bij het Landelijk Parket en in de regionale parketten, over gespecialiseerde officieren van justitie voor cybercrime. De komende jaren worden additionele middelen geïnvesteerd voor internationale samenwerking en om het verwerken van rechtshulpverzoeken bij het Openbaar Ministerie te versterken.

Voor een effectieve aanpak is bovendien de aanpassing van nationale wetgeving noodzakelijk. Daarom heeft de regering het Wetsvoorstel Computercriminaliteit III (Kamerstuk 34 372) aan het parlement gestuurd. De Tweede Kamer heeft het voorstel inmiddels aangenomen. Het wetsvoorstel behelst onder meer nieuwe strafbaarstellingen en bevoegdheden die nodig zijn voor een effectieve aanpak van cybercrime en de opsporing op internet. Voorts wordt op basis van de motie-Recourt van december 2016 (Kamerstuk 34 372, nr. 23) gewerkt aan een integraal plan van aanpak voor cybercrime.

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?

22. Antwoord van het kabinet:
Het kabinet is van mening dat spionage, waaronder digitale spionage, als zodanig niet expliciet is toegestaan of verboden onder het internationaal recht. Uitgangspunt bij het uitoefenen van de bevoegdheden van de inlichtingen- en veiligheidsdiensten is de Nederlandse wetgeving. Spioneren door buitenlandse mogendheden zonder dat wij daarvan weten is wettelijk niet toegestaan.

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?

23. Antwoord van het kabinet:
Een gezaghebbende studie van het United Nations Institute for Disarmament Research stelde dat 41 landen in 2013 publiekelijk erkenden dat zij beschikten over enige mate van militaire planning voor activiteiten in het cyberdomein of specifieke militaire cyber organisaties. Daaronder waren tenminste twaalf van de vijftien landen die het meest aan defensie uitgaven. Over

de mate waarin specifieke landen al dan niet transparant zijn kan het kabinet in het openbaar geen uitspraken doen.[3]

Nederland beschouwt transparantie als een vertrouwenwekkende maatregel die kan helpen om misverstanden te voorkomen en wantrouwen te verminderen. Dit kan een bijdrage leveren aan het bevorderen van de internationale stabiliteit, het voorkomen van het ontstaan van een wapenwedloop en het wegnemen van wantrouwen en gevaar op escalatie en miscalculatie.

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?

24. Antwoord van het kabinet:
In de kamerbrief van de Minister van Veiligheid en Justitie over kwetsbaarheden in hardware en software (Kamerstuk 26 643, nr. 428) meldt het kabinet dat om een zorgvuldige afweging te kunnen maken over de inzet van de genoemde bevoegdheden, elke bevoegdheid van wettelijke voorwaarden en waarborgen is voorzien. Dit geldt ook voor de ontwikkeling en inzet van offensieve cybercapaciteiten. Dat betekent ook dat wanneer een onbekende kwetsbaarheid wordt gevonden in een systeem en Nederlandse belangen daar hinder van kunnen ondervinden, deze kwetsbaarheid in principe gemeld zal worden. Is het een kwetsbaarheid in een wapensysteem van de tegenstander die we in Nederland niet kennen, dan kan het proportioneel zijn dat deze gebruikt wordt. Of het gebruik van een kwetsbaarheid de meest aangewezen methode is, wordt per geval bepaald.

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?

25. Antwoord van het kabinet:

[3] United Nations Institute for Disarmament Research, The Cyber Index: International Security Trends and Realities, 2013.

Het cyberbeleid komt tot stand door afstemming tussen de betrokken ministeries. Het Ministerie van Veiligheid en Justitie heeft een coördinerende rol op het gebied van cybersecurity. Uiteraard laat dit op het gebied van cybersecurity onverlet dat de genoemde departementen en diensten alle een specifieke rol en verantwoordelijkheid hebben op het gebied van cybersecurity. Daarbij verwijs ik u naar de beantwoording van vragen van het lid Recourt d.d. 14 augustus 2014 (Aanhangsel Handelingen II 2013/14, nr. 2703).

Het is niet aan dit kabinet om uitspraken te doen over de wijze waarop dit onderwerp onder een nieuw kabinet zal worden belegd.

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?

26. Antwoord van het kabinet:
De reactie op cyberoperaties door statelijke actoren hangt af van de aard en de impact van specifieke incidenten. Het kabinet kan hier van geval tot geval op reageren met een breed spectrum aan nationale en bondgenootschappelijke instrumenten. Het kabinet streeft er naar om dit instrumentarium verder te ontwikkelen.

Het kabinet benadrukt dat er reeds sprake is van een internationaalrechtelijk kader voor de regulering van cyberoperaties. Diverse landen, waaronder Nederland, hadden de toepasbaarheid van het bestaand internationaal recht op cyberoperaties reeds bevestigd, maar in de UN Group of Governmental Experts van 2013 werd hier ook in VN kader overeenstemming over bereikt. Er bestaat brede steun voor het verder uitwerken hoe specifieke regels moeten worden toegepast op cyberoperaties. Onder meer de huidige UN GGE probeert daar verdere vooruitgang op te boeken. Het kabinet probeert dat te ondersteunen, bijvoorbeeld door discussie over de Tallinn Manual 2.0 tussen juridisch adviseurs van een grote groep landen te faciliteren.

Voor wat betreft de officiële visie van andere landen op de rechtmatigheid van cyberoperaties verwijst het kabinet naar officiële publicaties daarover van deze landen.

Zijn landen verantwoordelijk voor het berechten van cybercriminelen die op hun grondgebied opereren en voor het verhalen van de schade die deze cybercriminelen toebrengen?

27. Antwoord van het kabinet:
Elk land is zelf verantwoordelijk voor verdachten die op hun grondgebied actief zijn met criminele activiteiten of dit nu drugscriminaliteit, mensenhandel of cybercriminaliteit betreft. Een ander land kan echter eveneens rechtsmacht en (grote) belangen hebben om criminaliteit te onderzoeken die effect heeft op zijn grondgebied.

Op het terrein van cybercriminaliteit doet zich in een overgroot deel van de strafrechtelijke onderzoeken een situatie voor waarbij er in diverse landen slachtoffers (burgers, bedrijven of overheden) zijn gemaakt door het plegen van computercriminaliteit, zoals computervredebreuk, het overnemen, aftappen of vernietigen van gegevens, DDos-aanvallen enz. In die situatie zullen veelal meerdere landen een strafrechtelijk onderzoek starten om te onderzoeken vanuit waar de aanval wordt gepleegd en wie daar mogelijk van kan worden verdacht. Die onderzoeken leiden wederom in het grootste deel van de gevallen naar landen waar weliswaar de infrastructuur staat waarmee de strafbare feiten (mede) worden gepleegd of aangestuurd, maar wat veelal niet de locatie is van de natuurlijke personen die achter deze strafbare feiten zitten.

Het nader onderzoeken van de identiteit van de verdachten die achter dergelijke strafbare feiten zitten, is tijdrovend, internationaal georiënteerd en technisch vaak zeer gecompliceerd door de eenvoudige beschikbaarheid van afschermingsmiddelen, zoals proxy's, Virtueel Privénetwerk (VPN) aanbieders, The Onion Router (TOR) (is een netwerk van servers waarin internet verkeer over de hele wereld wordt gerouteerd waardoor het zeer moeilijk is om de bron te achterhalen) en The Amnestic Incognito Live System (Tails) (systeem dat is gericht op privacy en anonimisering) software en anonieme betalingsmiddelen. Er staan de opsporingsinstituten weinig mogelijkheden ter beschikking om deze afschermingen te doorbreken, behalve het intensief samenwerken op internationaal niveau.

Indien er verdachten worden geïdentificeerd is het vervolgens afhankelijk van de wetgeving van het land waar deze personen verblijven of uitlevering/overlevering mogelijk is naar andere landen. Er zijn nog diverse landen die geen eigen onderdanen uitleveren en in die gevallen zal moeten worden bezien of het overdragen van de strafzaak een alternatief vormt. In sommige gevallen reist een verdachte ook over de grenzen en kan het wachten op een dergelijk scenario beter zijn.

In sommige zaken is het vragen van uitlevering of overlevering mogelijk en daar wordt nu reeds gebruik van gemaakt. In andere zaken wordt een inschatting gemaakt of het delen van informatie of het doen van rechtshulp leidt tot een aanhouding van verdachte. Indien het tot een vervolging komt is het vervolgende land als eerste verantwoordelijk voor het verhalen van de schade op de verdachte.

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?

28. Antwoord van het kabinet:
Zie antwoord 37 op de vragen van de leden van de SP-fractie.

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?

29. Antwoord van het kabinet:
Zie antwoord 10 op de vragen van de leden van de PVV-fractie.

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?

30. Antwoord van het kabinet:
De integratie van het cyberbeleid binnen het gemeenschappelijk buitenland- en veiligheidsbeleid heeft onder meer vorm gekregen in de EU Cyber Security Strategie uit 2013, het EU Cyber Defence policy framework uit 2014, de Raadsconclusies over Cyberdiplomatie uit 2015 en de EU Global Strategy uit 2016. Het kabinet maakt zich samen met de Europese Dienst voor Extern Optreden (EDEO), de Europese Commissie en andere lidstaten hard voor verdere intensivering van het gemeenschappelijke optreden op dit gebied.

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?

31. Antwoord van het kabinet:
De Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIB-richtlijn) bepaalt dat er een samenwerkingsgroep wordt opgericht, met daarin vertegenwoordigers van de EU lidstaten, de Commissie en het **Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA). Doel van samenwerkingsgroep is om de strategische samenwerking en de uitwisseling van informatie tussen de lidstaten te ondersteunen en te faciliteren, vertrouwen te scheppen, en een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie tot stand te brengen. De samenwerkingsgroep verricht haar taken op basis van tweejarige werkprogramma's.**

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

32. Antwoord van het kabinet:
De verantwoordelijk ligt uiteraard bij de deelnemende CSIRTs. Vertrouwen is immers essentieel bij operationele samenwerking. De Europese Netwerk- en Informatiebeveiligingsrichtlijn bepaalt dat alle landen in Europa dienen te beschikken over een goed functionerend CSIRT. Daarnaast wordt in deze richtlijn bepaald dat een CSIRT-netwerk wordt ingesteld, met daarin vertegenwoordigers van de CSIRTs van de lidstaten en CERT-EU. Dit netwerk heeft onder meer tot taak om vormen van operationele samenwerking te bespreken en waar mogelijk wederzijdse bijstand te verlenen bij de aanpak van grensoverschrijdende incidenten. Daarnaast werken CSIRTs ook thans al onder meer bilateraal samen.

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?

33. Antwoord van het kabinet:
Voor het antwoord op de vraag over het onderscheid tussen militaire en civiele cybercapaciteiten moet om te beginnen worden gekeken naar de (grondwettelijke) taken van de krijgsmacht en de middelen die zij voor de uitvoering daarvan heeft gekregen. De taken van de krijgsmacht liggen traditioneel en primair in het domein van internationale conflictbeheersing, waarbij de krijgsmacht de zwaardmacht heeft. De middelen van de krijgsmacht zijn in zijn algemeenheid – en zonder afbreuk te doen aan haar humanitaire taken – dan ook primair afgestemd op acteren in (gewapend) conflict, binnen het daarvoor vereiste (volkenrechtelijk) mandaat. Dat geldt ook voor de samenstelling en inzet van militaire cybercapaciteiten.

Dit laat echter onverlet dat die capaciteiten – evenals de andere capaciteiten van de krijgsmacht – binnen de vigerende civiele juridische kaders beschikbaar kunnen worden gesteld aan (nationale) civiele autoriteiten ten behoeve van crisisbeheersing, rampenbestrijding en rechtshandhaving; ook wel de derde hoofdtaak van de krijgsmacht genoemd. In spiegelbeeld: de cybercapaciteiten van civiele uitvoeringsorganisaties zijn op de laatstgenoemde doeleinden gericht, niet op het uitoefenen van de zwaardmacht ten behoeve van (internationale) conflictbeheersing.

In de kamerbrief over cybersamenwerking tussen EU en NAVO (Kamerstuk 33 321, nr. 8) heeft het kabinet gemeld dat de taken en verantwoordelijkheden van EU en NAVO verschillend zijn, maar voor een deel wel complementair. De ordenende rol van EU en de veiligheidsbevorderende rol van NAVO kunnen elkaar versterken waardoor ook afzonderlijke ambities beter verwezenlijkt kunnen worden.

Ten aanzien van de rol van NAVO in het cyberdomein is tijdens de top in Wales in 2014 besloten dat «cyber» onderdeel uitmaakt van de collectieve verdediging. Een cyberaanval kan het niveau van een gewapende aanval bereiken en kan dus ook tot een collectieve reactie leiden.

Tevens is tijdens de top in Warschau in 2016 cyberspace als domein erkend. Dat houdt in dat alle cyberelementen vanaf nu in het operationele proces worden geïntegreerd. Naast de technische verdediging van de netwerken, worden cyberelementen bijvoorbeeld voortaan ook meegenomen in het opstellen van een dreigingsbeeld door middel van inlichtingen en bij het plannen van een operatie.

De uitwerking van de genomen besluiten vindt op dit moment plaats en is uitgeschreven in de «roadmap to implement cyberspace as a domain of operations» van de NAVO. In deze roadmap zijn tien «lines of effort» gedefinieerd. Binnen drie jaar moeten de studies die zijn of worden opgestart in het kader van de roadmap voltooid zijn.

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?

34. Antwoord van het kabinet:
Deze kwesties gaan Duitsland aan. Indien geconstateerd wordt dat een buitenlandse mogendheid zonder toestemming inlichtingenactiviteiten verricht op Nederlands grondgebied, treft de Nederlandse regering maatregelen.

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?

35. Antwoord van het kabinet:
Exportcontrole is een belangrijk instrument om onder andere proliferatie en verkeerd gebruik van goederen, waaronder cybertechnologie tegen te gaan. Internationaal wordt samengewerkt in een aantal exportcontroleregimes en is op EU-niveau regelgeving vastgesteld in o.a. de Verordening tot instelling van een communautaire regeling voor controle op de uitvoer, de overbrenging, de tussenhandel en de doorvoer van producten voor tweeërlei gebruik (EU 428/2009).

De Europese Commissie heeft in september 2016 een voorstel gedaan voor de herziening van de bestaande verordening met het doel deze te moderniseren en beter aan te laten sluiten op de internationale ontwikkelingen. De Europese Commissie stelt een aantal wijzigingen voor. Zo stelt de Commissie voor om de controle van export van cybertoezichttechnologie te intensiveren in relatie tot mensenrechtenschendingen. Voorbeelden van dergelijke cybertoezichttechnologie zijn goederen die internetgegevens kunnen monitoren en digitale communicatie of informatie kunnen onderscheppen.

Nederland is voorstander van het uitbreiden van de al bestaande controle op apparatuur voor cybertoezicht met het voorkomen van mensenrechtenschendingen als grondslag (in aanvulling op proliferatie van massavernietigingswapens). De EU loopt daarmee wereldwijd voorop en het sluit aan bij de al bestaande Nederlandse praktijk waarbij mensenrechten als criterium voor exportcontrole wordt toegepast.

De Nederlandse inzet gaat daarbij uit van drie elementen: 1) exportcontrole vindt plaats aan de hand van lijsten met gedefinieerde goederen, zoals vastgesteld in de exportcontroleregimes; 2) de mogelijkheid tot inzet van een instrument van ad hoc-vergunningplicht als controle-instrument voor specifieke casussen; 3) inzet op samenwerking met het bedrijfsleven vanuit het principe van maatschappelijk verantwoord ondernemen.

De Europese Commissie stelt voor de definitie van goederen voor tweeërlei gebruik uit te breiden en de wereldwijd gebruikte controlelijsten voor de EU uit te breiden met een separate EU controlelijst voor de categorie goederen die ingezet kunnen worden bij het schenden van mensenrechten. Nederland staat vooral vanuit praktisch oogpunt kritisch tegenover deze uitwerking: het creëren van een separate definitie in de EU en

een controlelijst die niet in overeenstemming is met de verschillende lijsten van exportcontroleregimes, kan leiden tot intransparantie, dubbelingen of juist tegenstrijdigheden als gevolg van externe ontwikkelingen binnen deze regimes. Dat kan tot onduidelijkheid leiden voor het bedrijfsleven. Een aandachtspunt daarbij is het voorkomen van een onevenredige verstoring van het gelijk speelveld op mondiaal niveau.

Nederland steunt het voorstel van de Commissie om de dual-useverordening te moderniseren en te vernieuwen, inclusief de verdere verankering van mensenrechten als grondslag voor exportcontrole. Hierbij zal Nederland de uitwerking toetsen aan praktische toepasbaarheid en uitvoerbaarheid, impact op het wereldwijd gelijk speelveld en administratieve lasten en beveiligingsonderzoekers en incident responders, zoals CSIRTs. Ook is Nederland zich er van bewust dat de regelgeving defensieve inzet van cybertoezichttechnologie niet onnodig zou moeten hinderen.

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?

36. Antwoord van het kabinet:
De cyberdreiging die uitgaat van statelijke actoren, wordt beschreven in de ICS, het jaarlijkse Cyber Security Beeld Nederland (CSBN) en de jaarverslagen van de inlichtingen- en veiligheidsdiensten. Het kabinet verwijst dan ook naar deze documenten.

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?

37. Antwoord van het kabinet:
In antwoord op de door de leden van de fracties van de PVV, Groen Links en de SP gestelde vragen over de mate waarin Nederland voorbereid is op de digitale dreiging, de opbouw van capaciteiten en de financiële kaders kan worden aangegeven dat het antwoord op de dreiging wordt uitgewerkt aan de hand van de opeenvolgende nationale cybersecurity strategieën. Deze behelzen de door de fractie Groen Links gevraagde robuuste capaciteit. Daarnaast zal de implementatie van de Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIB-richtlijn), met daarin onder meer verplichtingen voor vitale aanbieders om adequate beveiligingsmaatregelen te nemen, ernstige incidenten te melden, en toezicht op de naleving hiervan, verder kunnen bijdragen aan het verhogen van de digitale weerbaarheid van vitale infrastructuren. Voorts zij gewezen op het wetsvoorstel

gegevenswerking en meldplicht cybersecurity, dat daarop vooruitlopend onder meer voorziet in een meldplicht bij het Nationaal Cyber Security Centrum (NCSC) voor vitale aanbieders van ernstige incidenten.

Gezien de huidige dreiging, zoals aangegeven in het Cyber Security Beeld Nederland (CSBN) 2016 en de jaarverslagen van de inlichtingen- en veiligheidsdiensten, heeft het kabinet in 2016 additioneel geïnvesteerd in cybersecurity. In de beleidsreactie op het CSBN 2016 heeft het kabinet aangegeven dat de doorontwikkeling van de Nederlandse cybersecurity noodzakelijk is als gevolg van de kwantitatief en kwalitatief toenemende dreiging in combinatie met een toenemende afhankelijkheid van inherent kwetsbare ICT in Nederland. Uiteraard zijn aanbieders in vitale sectoren zelf primair verantwoordelijk voor de eigen investeringen om netwerkinbreuken te voorkomen en te adresseren. Door het NCSC wordt ervoor gezorgd dat deze aanbieders over dreigingen worden geïnformeerd en geadviseerd, en kan ook overigens ondersteuning worden verleend om de uitval van voor de samenleving vitale diensten te voorkomen of beperken.

Voor een volledig overzicht van de inspanningen kan worden verwezen naar de beleidsreactie van het kabinet op het CSBN 2016 (Kamerstuk 26 643, nr. 420).

In ieder geval kan worden aangegeven dat in de begroting van het Ministerie van Veiligheid en Justitie van 2017 besloten is om voor nu, in 2017 5 miljoen euro en vanaf 2018 structureel 14 miljoen euro additioneel beschikbaar te maken voor cybersecurity en de aanpak van cybercriminaliteit. Onderdeel hiervan is het Nationaal Detectie Netwerk waarin het NCSC, de AIVD en MIVD samenwerken om cyberaanvallen op rijksoverheid en vitale infrastructuur te onderkennen, zodat deze aanvallen sneller aangepakt kunnen worden en de effecten ervan beheersbaar worden gemaakt. Naast de structurele inzet in de begroting van het Ministerie van Veiligheid en Justitie en bovenstaande additionele impuls komt cybersecurity tevens terug in andere delen van de Rijksbegroting. Dit betreft bijvoorbeeld de generieke budgetten die worden aangewend voor ICT. Verdere intensivering, onder andere voor het versterken van internationale partnerschappen en coalities, is aan een volgend kabinet.

In antwoord op de door de SP gestelde vraag over de inzet van de afgelopen 10 jaar wordt verwezen naar de opeenvolgende voortgangsbrieven behorende bij de twee strategieën, waarin de inzet van het kabinet aangaande cybersecurity is vastgelegd.
In reactie op de vraag van het lid van de PVV-fractie inzake grootschalige oefeningen kan worden opgemerkt dat zowel nationaal als internationaal oefeningen georganiseerd worden. Nederland organiseert een keer in de twee jaar een nationale oefening met samenwerkingspartners, afkomstig uit zowel de publieke als private sector.
Daarnaast neemt het NCSC deel aan een Europese oefening onder de naam Cyber Europe. Tevens heeft Defensie met het Defensie Cyber Commando (DCC) en het Defensie Computer Emergency and Response Team (DefCERT) bijgedragen aan internationale oefeningen, zoals Cyber Coalition, Locked Shields en Trident Jaguar. Ook het Ministerie van Buitenlandse Zaken neemt deel aan strategische en cyberdiplomatieke oefeningen in internationale organisaties, bijvoorbeeld binnen de NAVO en de OVSE.

Wat de vragen van de fractie Groen Links over gekwalificeerd personeel en de vullingsgraad van de vacatures bij het NCSC betreft, kan worden opgemerkt dat het NCSC op dit moment voldoende gekwalificeerde mensen in dienst heeft.
Het NCSC heeft tot op heden geen grote problemen ondervonden bij het vinden van het juiste personeel. Thans is sprake van een personele uitbreiding gaande van 19 fte's ten behoeve van de activiteiten in het kader van het Nationaal Detectienetwerk.

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?

38. Antwoord van het kabinet:
Het cyberdomein biedt veel mogelijkheden tot anonimiteit en heimelijkheid. De technologie hiervoor is vaak gemakkelijk verkrijgbaar en vergt kleine investeringen. Voorbeelden zijn The Onion Router (TOR) en encryptiesoftware. Ook kan gebruik worden gemaakt van zogenaamde bullet proof hosting, waarbij hostingbedrijven illegale activiteiten faciliteren en deze activiteiten zo veel mogelijk afschermen van rechtmatige onderzoeken door overheden. Dergelijke mogelijkheden worden vaak gecombineerd met het routeren van internetverkeer door diverse landen. Overheden en technisch vaardige criminelen hebben vaak nog uitgebreidere mogelijkheden om hun activiteiten en locatie te verbergen. Deze mogelijkheden maken attributie in veel gevallen zeer lastig. Internationale samenwerking is daarom van cruciaal belang om cyberaanvallen en cybercriminaliteit tegen te gaan. Over het belang van internationale samenwerking in de opsporing is reeds in gegaan bij vraag 21 en zal verder worden benadrukt in antwoord op vraag 48.

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?

39. Antwoord van het kabinet:
De Nederlandse regering past terughoudendheid bij het reageren op de stukken die door Wikileaks zijn gepubliceerd en die een ander land betreffen.

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?

40. Antwoord van het kabinet:
Het kabinet heeft geen reden om aan het oordeel van de Verenigde Staten over de toerekening van de desbetreffende cyberoperaties te twijfelen.

Voor zover senator McCain met deze uitspraak bedoelde dat het beïnvloeden van verkiezingsprocessen gelijk staat aan het gebruik van geweld of uitvoeren van een gewapende aanval, deelt het kabinet die analyse niet. Dat neemt niet weg dat het kabinet, net als senator McCain, pogingen tot dergelijke beïnvloeding zeer ernstig opneemt.

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?

41. Antwoord van het kabinet:
De AIVD en de MIVD richten zich op cyberdreigingen gericht tegen Nederland en Nederlandse belangen. Over deze onderzoeken kan het kabinet in de openbaarheid geen uitspraken doen.

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?

42. Antwoord van het kabinet:
Het kabinet maakt zich zorgen over de mogelijkheden van het cyberdomein en cybercapaciteiten om de Nederlandse nationale veiligheid te bedreigen. Er bestaan aanzienlijke verschillen in de visies van verschillende landen op internationale veiligheid in het cyberdomein. Dit is een complicerende factor in de internationale onderhandelingsprocessen, die zich nog in een relatief vroeg stadium bevinden en veel tijd zullen vragen. Gezien de urgentie van de problematiek en onze grote belangen blijft Nederland echter druk zetten, onder meer door initiatieven te ontplooien die gericht zijn op het bevorderen van kennisopbouw en dialoog en door coalities te vormen met gelijkgestemden. De inzet van het kabinet is er onder andere op gericht om een normatief kader te bewerkstelligen voor de regulering van cyberoperaties door

statelijke actoren. Het kabinet is van mening dat het bestaande internationaal recht voldoende basis is voor dit normatieve kader. Het kabinet streeft dan ook niet naar nieuwe regelgeving op dit gebied, maar naar verheldering van de toepassing van bestaande regels.

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?

43. Antwoord van het kabinet:
Zoals de regering aangaf in de kabinetsreactie op het AIV/CAVV advies Digitale Oorlogvoering (Kamerstuk 33 000 X, nr. 79) is op cyberaanvallen hetzelfde internationaalrechtelijke kader van toepassing als op fysieke aanvallen. Dat kader en de grondslagen voor het interstatelijk gebruik van geweld, waaronder cyberaanvallen, is door de regering uiteengezet in onder andere de brief van de Minister van Buitenlandse Zaken van 1 oktober 2014 (Kamerstuk 27 925, nr. 518). Kort samengevat acht de regering drie uitzonderingen van toepassing voor het overigens geldende geweldverbod in de internationale betrekkingen zoals dat is vastgelegd in artikel 2, vierde lid, van het Handvest van de Verenigde Naties. De eerste uitzondering betreft een verzoek of toestemming van een derde Staat om in die Staat geweld te gebruiken, uiteraard voor zover dat verzoek in overeenstemming is met het internationale recht. De tweede uitzondering is een resolutie van de VN Veiligheidsraad op basis van Hoofdstuk VII van het Handvest van de Verenigde Naties. De derde en laatste uitzondering is het optreden, onder toepassing van de eisen van noodzakelijkheid en proportionaliteit, op basis van nationale of collectieve zelfverdediging in reactie op een (onmiddellijk dreigende) gewapende aanval door een andere Staat of een georganiseerde gewapende groep.

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?

44. Antwoord van het kabinet:
Op de punten waar het kabinet pleit voor meer transparantie is Nederland reeds open: in de Defensie Cyber Strategie (Kamerstuk 33 321, nr. 2) en de actualisatie van de Defensie Cyber Strategie (Kamerstuk 33 321, nr. 5) gaat het kabinet in op de doelen waartoe cybercapaciteiten dienen. Zie verder antwoord 23 en antwoord 43.

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?

45. Antwoord van het kabinet:
De continue stroom aan internationaal dataverkeer zal naar verwachting in de toekomst nog groter worden. Het verwerken van persoonsgegevens en de bescherming van de persoonlijke levenssfeer is in Nederland aan strikte normen en toezicht gebonden, mede op basis van Europese wetgeving. Internationale juridische kaders zijn noodzakelijk wanneer er gegevensuitwisseling plaatsvindt met landen die lagere standaarden hanteren dan Nederland en in Europees-verband.

In internationaal en Europees-verband trekt Nederland op met staten die het belang van een adequate bescherming van persoonsgegevens en persoonlijke levenssfeer van eveneens onderschrijven. De Nederlandse wettelijke kaders fungeren hierbij als uitgangspunt alsmede, Europese en internationale verplichtingen. Binnen deze kaders werkt Nederland samen met internationale partners, zoals de VS.

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?

46. Antwoord van het kabinet:
Nederland streeft naar internationale waarborgen voor een open, vrij en veilig internet. Uitgangspunt daarbij is het het multistakeholdermodel van «internet governance» waarbij onderzoeksinstituten, standaardisatie- en technische organisaties, bedrijfsleven, maatschappelijk middenveld, gebruikersorganisaties en overheden gezamenlijk werken aan de ontwikkeling en het beheer van het internet. In lijn daarmee bepleit Nederland in de daartoe geëigende fora zoals de UN Group of Governmental Experts (UN GGE) verankering van de erkenning dat internationaal recht van toepassing is in het cyberdomein.

Daarnaast kunnen vrijwillige gedragsnormen en vertrouwenwekkende maatregelen worden afgesproken in aanvulling op het internationaal recht. Om ervoor te zorgen dat de standpunten van relevante stakeholders in het internet naar behoren worden meegewogen bij internationale overleggen over het borgen van veiligheid en stabiliteit in het cyberdomein, steunt de regering

initiatieven zoals de Global Commission on the Stability of Cyberspace (GCSC). De GCSC bestaat uit deskundigen vanuit overheid, bedrijfsleven, technische gemeenschap, academici en civil society samen. Gezamenlijk ontwikkelen deze deskundigen voorstellen voor gedragsnormen en andere beleidsinitiatieven.

Bij nieuwe maatregelen en gedragsnormen is de inzet dat deze juist complementair en aanvullend zijn ten aanzien van de bestaande zelforganisatie en -regulering binnen het internet, en deze niet onnodig beperken of aantasten.

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?

47. Antwoord van het kabinet:
Ja. Het kabinet verwijst hierbij naar de memorie van toelichting bij het wetsvoorstel en de nota naar aanleiding van het verslag van de Vaste Commissie Binnenlandse Zaken van de Tweede Kamer.

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?

48. Antwoord van het kabinet:
Vanwege de afwezigheid van grenzen in cyberspace, de mogelijkheden voor anonimiteit en de mogelijkheden om het zeer lastig te maken een geografische plaats van elektronisch bewijs of de oorsprong van een cyberaanval te achterhalen, is het vaak praktisch niet mogelijk de fysieke locatie waar gegevens zijn opgeslagen, worden verwerkt of overgedragen te achterhalen. Door de grenzeloosheid van het internet zijn de mogelijkheden voor criminelen om gegevens en activiteiten snel te verplaatsten en voor de opsporing te verbergen groot, zeker in vergelijking met de op territorialiteit gebaseerde procedures voor internationale opsporing. Vooral in situaties waarin gegevens over strafbare feiten snel worden verplaatst of wanneer het redelijkerwijs niet mogelijk is de fysieke plaats van gegevens te achterhalen, zijn de traditionele mogelijkheden voor internationale opsporing ontoereikend. In juni 2016 heeft de JBZ-raad daarom conclusies aangenomen over criminal justice in cyberspace. Deze conclusies zien op:
- **het ontwikkelen van een gezamenlijk EU kader voor verzoeken aan private partijen voor het verkrijgen van bepaalde typen data. Hierbij wordt gestreefd naar synergie met de formulieren**

en instrumenten die binnen de EU voor rechtshulp al eerder zijn ontwikkeld en gangbaar zijn;
- **het stroomlijnen en versnellen van de bestaande procedures voor wederzijdse rechtshulp (mutual legal assistance, MLA) en wederzijdse erkenning (mutual recognition) binnen de EU en met derde landen, onder andere door digitalisering van verzoeken en automatische vertaling hiervan, als ook het vergroten van kennis en vaardigheden van hen die in de lidstaten deze verzoeken behandelen;**
- **het herijken van de afspraken ten aanzien van handhavende rechtsmacht («enforcement jurisdiction») door te bezien welke onderzoekshandelingen onder welke voorwaarden mogen worden ingezet in cyberspace, in de gevallen waarin het huidige kader nog niet voorziet, onder andere wanneer de locatie van elektronisch bewijs of de oorsprong van een cyber aanval (nog) niet bekend of redelijkerwijs niet bekend te maken is.**

In vervolg op de raadsconclusies wordt onder regie van de Commissie, in nauwe samenwerking met lidstaten en met andere zowel nationale als Europese instituties, uitvoering gegeven aan de in de raadsconclusies genoemde actiepunten. In de raadsconclusies wordt de Commissie verzocht resultaten van het proces inzake handhavende rechtsmacht te rapporteren aan de JBZ-raad in juni 2017.

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?

49. Antwoord van het kabinet:
Het kabinet zet zich op de middellange en lange termijn in voor een normatief kader. Er wordt geïnvesteerd in het verhelderen van de toepassing van het internationaal recht, ontwikkelen en operationaliseren van vrijwillige niet-bindende gedragsnormen en vertrouwenwekkende maatregelen met betrekking tot het internet en de toegankelijke diensten en toepassingen. Het bestaande internationaal recht is voldoende als basis voor dit normatieve kader en er wordt dan ook niet gestreefd naar nieuwe regelgeving op dit gebied, maar naar verheldering van de toepassing van bestaande regels. Het decentrale karakter van het internet impliceert dat deze afspraken binnen een multistakeholder aanpak worden gemaakt tussen staten, private actoren, het maatschappelijk middenveld, de academische wereld en technische gemeenschap. Een voorbeeld hiervan is de slotverklaring van de mondiale multistakeholder internetconferentie NETmundial van 24 april 2014. Deze slotverklaring bevat gemeenschappelijk aanvaarde internetprincipes, zoals de vrijheid van meningsuiting en het recht op privacy, en een roadmap voor de ontwikkeling en het beheer van het internet. De Minister van Economische Zaken heeft de Kamer per brief van 26 juni 2014 over deze slotverklaring geïnformeerd (Kamerstuk 33 896, D).

Het kabinet blijft zich inzetten om zijn visie uit te dragen in verschillende gremia en coalities te bouwen om andersdenkenden

te overtuigen. Op 7 april jl. hebben ook de G20 landen in een ministeriële verklaring hun steun uitgesproken voor multistakeholder processen en initiatieven om een digitaal verbonden wereld te bereiken. Nederland, als gastdeelnemer aan G20, heeft in de discussies een dergelijke aanpak uitgedragen.

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?

50. Antwoord van het kabinet:
Stabiliteit in cyberspace is geen zaak van staten alleen. Bedrijven en academici zijn belangrijke spelers, het internet is immers merendeels in private handen. Nederland werkt daarom ook in multistakeholder verband samen. Bovendien is er verschillende regelgeving om te voorkomen dat bedrijven met een sterke marktpositie hun positie misbruiken. Zo verbiedt het mededingingsrecht bedrijven om misbruik te maken van hun economische machtspositie, bijvoorbeeld door concurrenten uit te sluiten of consumenten uit te buiten. Wanneer er sprake is van machtsmisbruik in mededingingsrechtelijke zin, is de Autoriteit Consument en Markt (ACM) bevoegd op te treden.

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

51. Antwoord van het kabinet:
Zie antwoord 10 op de vragen van de leden van de PVV-fractie.

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?

52. Antwoord van het kabinet:
Op basis van de conclusies van de JBZ-raad van juni 2016 is het Europese netwerk van officieren van justitie voor cybercrime gestart. Het netwerk faciliteert de operationele samenwerking en de uitwisseling van «best practices». Op 24 november 2016 heeft de startbijeenkomst plaatsgevonden. Er zijn na het besluit van de JBZ Raad inmiddels 2 vergaderingen gevolgd. In deze vergaderingen is besproken met welke onderwerpen en zaken het netwerk zich bezig zal houden. De gedachten daarover van de diverse Lidstaten zijn vervolgens uitgewerkt in een werkprogramma dat besproken is met diverse EU instanties en agentschappen, waaronder de Europese Commissie, de Raad, Europol en het Europees Justitieel Netwerk. Het werkprogramma is in de laatste vergadering vastgesteld door het netwerk en bevat activiteiten op het gebied van kennisdeling, opleiding en samenwerking met relevante actoren. Prioritaire onderwerpen zijn data retentie, encryptie en elektronisch bewijs. Het EJCN draagt reeds bij aan de activiteiten van de Commissie op deze onderwerpen.