“Digitaal bruggen slaan”

Internationale Cyberstrategie

naar een geïntegreerd internationaal cyberbeleid

1. Inleiding

Nederland zet in op een open, veilig en vrij cyberdomein. Hierin worden kansen die digitalisering onze economie en samenleving biedt volop benut, dreigingen worden het hoofd geboden en fundamentele rechten en waarden worden beschermd. Gezien het grensoverschrijdende karakter van het cyberdomein vergt het waarborgen van deze belangen ook internationale inspanning. Hoe Nederland zich internationaal inzet is van directe invloed op de positionering van Nederland als gidsland, vestigingsland en partnerland.

Met deze Internationale Cyberstrategie geeft het kabinet invulling aan de toezegging vervat in de kabinetsreactie op het advies van de AIV 'Het Internet, een wereldwijde vrije ruimte met begrensde staatsmacht' en de WRR 'De publieke kern van het Internet: naar een buitenlands internetbeleid'. De internationale cyberstrategie is complementair aan en in lijn met de Nationale Cyber Security Strategie (NCSS 2), de Digitale Agenda 2016-2017, de Mensenrechtenstrategie 2, de Defensie Cyber Strategie en de Nederlandse Internationale Veiligheidsstrategie.

Leeswijzer
In hoofdstuk 2 zijn de internationale belangen, dreigingen en uitdagingen weergegeven en zijn op basis daarvan de visie en uitgangspunten geformuleerd. In hoofdstuk 3 zijn de verschillende werkterreinen van internationale samenwerking op het gebied van cyberbeleid uiteengezet en zijn perspectieven voor verdere beleidsontwikkeling weergegeven. In hoofdstuk 4 zijn de beleidsprioriteiten uiteengezet om de sterke uitgangspositie van Nederland op het cyberdomein verder te versterken.

2. Belangen en visie

Naast de internationale belangen in het cyberdomein, bestaan er ook internationale dreigingen en uitdagingen. Op basis hiervan zijn de visie en uitgangspunten van beleid aansluitend in dit hoofdstuk weergegeven.

2.1 Internationale belangen

Het kabinet onderscheidt voor Nederland in internationale context een aantal fundamentele belangen met betrekking tot het cyberdomein. Zoals gesteld in de NCSS 2 beziet het kabinet deze belangen in een samenhang met vrijheid, veiligheid en groei.

2.1.1 Maatschappelijke en Economische Groei

Belang: Nederland is in staat de kansen die wereldwijde digitalisering onze samenleving en economie biedt te grijpen en deze verder te benutten
Nederland is een van de meest verbonden landen ter wereld met een concurrerende markt voor datacenters en hostingproviders. Daarmee is het uitstekend gepositioneerd om te profiteren van digitalisering. In Nederland levert informatie- en communicatietechnologie (ICT) een relatief grote bijdrage aan economische groei en wordt het in alle economische en maatschappelijke sectoren in toenemende mate toegepast. De Nederlandse samenleving ontwikkelt zich als gevolg hiervan tot een digitale kennis- en informatiesamenleving.

Belang: Nederland heeft baat bij een open, ongefragmenteerd Internet, waarin informatie vrij kan bewegen
Open governance en *permissionless innovation* zijn cruciaal voor de ontwikkeling van het internet. Mede door effectieve zelforganisatie en zelfregulering kon het internet uitgroeien tot een wereldwijd gedeelde en voor iedereen toegankelijke infrastructuur. Nederland wil internationaal de ontwikkeling, de openheid, de beschikbaarheid, de betrouwbaarheid, de veiligheid en de integriteit van het internet blijven waarborgen.

2.1.2 Fundamentele rechten en vrijheden

Belang: Nederland heeft baat bij een wereldwijde bescherming van mensenrechten online

Fundamentele rechten en vrijheden worden internationaal zowel offline als online alom erkend. Deze staan aan de basis van een open, vrije en veilige samenleving. Nederland beschouwt veiligheid en vrijheid niet als tegengestelde, maar als complementaire belangen: een veilige samenleving is een samenleving waarin de fundamentele rechten en vrijheden van het individu worden beschermd. Het bevorderen van een veilige digitale omgeving kan juist de rechten van mogelijk kwetsbare of bedreigde individuen beschermen. Het is van belang voor allen die zich in Nederland bevinden en die zich op het internet begeven dat deze rechten ook in de rest van de wereld goed worden beschermd en dat afspraken worden nageleefd.

2.1.3 Veiligheid

In het cyberdomein is veiligheid zowel een voorwaarde voor het functioneren van onze samenleving als een fundament van vertrouwen in onze economie en in de bescherming van rechten in het cyberdomein. Het kabinet onderscheidt op dit vlak drie veiligheidsbelangen:

Belang: Nederlandse burgers en bedrijven worden beschermd tegen cybercrime

Cybercrime is grensoverschrijdend en voor Nederland komt de dreiging vaak uit het buitenland. Om burgers en bedrijven in Nederland te beschermen is dan ook een stevige gecoördineerde internationale inzet nodig. Om de rechtsstaat ook in het cyberdomein te kunnen handhaven heeft Nederland er belang bij dat operationele samenwerking, opsporing en vervolging internationaal goed geregeld zijn.

Belang: Nederland is door internationale samenwerking weerbaar tegen verstoring, uitval of misbruik van ICT

Een open, vrij en stabiel cyberdomein kan niet worden gegarandeerd zonder veiligheid. Nederland zet zich daarom zowel nationaal als internationaal in voor de bevordering van cybersecurity.

Belang: *Nederland verdedigt zijn nationale veiligheidsbelangen samen met zijn internationale bondgenoten om vrede, veiligheid en stabiliteit te garanderen in het cyberdomein*

De drie strategische belangen uit de Internationale Veiligheidsstrategie zijn ook onverminderd in het cyberdomein van toepassing:

- verdediging van het eigen en bondgenootschappelijk grondgebied;
- een effectief functionerende internationale rechtsorde;
- economische veiligheid.

Deze belangen kennen allemaal een significante digitale component en lopen risico's door cyberdreigingen.

2.2 Internationale dreigingen

Verschillende kwaadwillende actoren maken steeds meer gebruik van het cyberdomein om hun belangen na te streven, bijvoorbeeld voor geldelijk gewin, het verwerven van informatie of politiek-militaire doeleinden. Deze trends en ontwikkelingen zijn onder meer in het jaarlijkse rapport Cyber Security Beeld Nederland (CSBN) uitgebreid geschetst.

Dreiging: Cybercrime vanuit het buitenland is zowel kwantitatief als kwalitatief een forse bedreiging voor de Nederlandse samenleving

De Nederlandse economie lijdt schade als gevolg van cybercriminaliteit en economische cyberspionage. Criminelen maken steeds vaker gebruik van het cyberdomein en zijn goed georganiseerd, waardoor de schade van criminele activiteiten op internet toeneemt.

Deze ontwikkelingen worden versterkt door de relatief lage kosten en risico's voor de plegers van cybercriminaliteit of cyberspionage. Bovendien zijn de kosten voor een sterke verdediging over het algemeen veel hoger dan voor het plegen van een digitale aanval.

Dreiging: Statelijke actoren gebruiken digitale middelen voor geopolitieke belangen en bedreigen de Nederlandse nationale veiligheid
Statelijke actoren zetten steeds meer digitale middelen in voor spionage-, beïnvloedings- en sabotagedoeleinden als integraal onderdeel van hun machtsinstrumentarium of concreet in conflictsituaties. De ontwikkeling van de dreiging kan niet los gezien worden van geopolitieke ontwikkelingen. De mogelijke rol van Rusland in de hacks tijdens de Amerikaanse verkiezingen is hiervan een voorbeeld. Rondom Europa hebben al dan niet 'hybride' conflicten een significante digitale component gekregen, zoals het geval is in Oekraïne en Syrië. Bestaande en sluimerende conflicten verplaatsen zich bovendien naar het cyberdomein. Nederland is reeds structureel slachtoffer van digitale inlichtingenactiviteiten. De Nederlandse overheid, ministeries maar ook bedrijven, zijn structureel doelwit van digitale spionageaanvallen. Het is waarschijnlijk dat dergelijke aanvallen tegen Nederland tijdens oplopende geopolitieke spanningen in omvang en intensiteit toenemen. Dit geldt met name wanneer dergelijke spanningen Nederland raken.

Dreiging: Het toenemende gebruik van cyberoperaties voor politieke doeleinden bedreigt de internationale rechtsorde
De attributie van internationale onrechtmatige daden en de verificatie van de naleving van bestaande regels is moeilijk toepasbaar in het cyberdomein en cyberoperaties bedreigen daarmee de internationale rechtsorde. Cyberoperaties bieden mogelijkheden om dwingende effecten te creëren die onder traditionele juridische drempels van het VN Handvest en NAVO Artikel 5 blijven. Bovendien vinden deze operaties vaak plaats buiten het publieke zicht en bewustzijn.

Dreiging: Cyberaanvallen op vitale infrastructuren door internationale actoren kunnen een ernstige bedreiging vormen voor de nationale veiligheid door manipulatie, ontzegging van of schade aan systemen
Uiteenlopende onderdelen van de (rijks)overheid werken samen om cyberaanvallen op de rijksoverheid en vitale infrastructuren tijdig te onderkennen, te bestrijden en de effecten ervan beheersbaar te maken. Dit kan niet zonder nauwe samenwerking met private partners, die veelal in nationale en internationale ketens verbonden zijn. De bewustwording en weerbaarheid van alle partners is essentieel.

Dreiging: Digitale economische spionage door buitenlandse inlichtingendiensten zet de concurrentiepositie van Nederland onder druk
Het afgelopen jaar zijn veel digitale aanvallen waargenomen op bedrijven in Nederland, waarbij het motief economische spionage was. Spionage met een economisch oogmerk is schadelijk voor de concurrentiepositie van Nederland. Deze aanvallen richtten zich op het verkrijgen van technologie die zijn marktwaarde soms nog moet bewijzen. De technologieën en bedrijfsgeheimen die worden ontvreemd kunnen van grote waarde zijn voor een stabiele en groeiende economie die de basis vormt van onze welvaart. Twee derde van de getroffen bedrijven had deze aanvallen niet zelf waargenomen.

2.3 Internationale uitdagingen
Naast de dreigingen zijn er ook een aantal ontwikkelingen waarmee rekening dient te worden gehouden. Hoewel ontwikkelingen op digitaal gebied zich lastig laten voorspellen, zijn er wel een aantal nu al relevante internationale uitdagingen te identificeren:
- *De hoeveelheid data neemt alleen maar toe, zowel nationaal als internationaal;* de internationale interesse in het verkrijgen van die data ook. De publieke en private sector werken steeds meer

data driven met grote databestanden die in toenemende mate in de *cloud* en daarmee vaak ook buiten de landsgrenzen worden opgeslagen.
- *Het internet der dingen (alles is verbonden aan het internet) en hyperconnectiviteit (alles en iedereen worden met elkaar verbonden)* bevorderen innovatie en brengen veel gebruikersgemak met zich mee, maar zorgen ook voor mogelijkheden tot misbruik op wereldwijde schaal.
- *Het jurisdictievraagstuk bemoeilijkt de opsporing en vervolging van cybercrime en de bescherming van burgers, en schaadt het vertrouwen van de samenleving in het cyberdomein.* Ook in het cyberdomein is het de taak van de overheid om recht te handhaven. Het wereldwijde karakter van het cyberdomein verhoudt zich echter slecht met de territoriale grenzen van 'klassieke' nationale jurisdictie. De opsporing van strafbare feiten gaat uit van territoriale jurisdictie voor handhaving en toepassing van opsporingsmethoden. Doordat 'klassieke' jurisdictie niet volledig van toepassing is op het cyberdomein wordt opsporing ernstig bemoeilijkt en criminelen profiteren hiervan. Het gebruikelijke systeem van internationale rechtshulp is zeer traag in vergelijking met de snelle ontwijkingsmogelijkheden die criminelen benutten. Het cyberdomein dreigt hierdoor voor technisch vaardige criminelen een vrijplaats te worden voor het plegen van strafbare feiten.
- *Het decentrale en anonieme karakter van het internet bemoeilijkt het handhaven en controleren van gemaakte afspraken*. Het cyberdomein biedt bij uitstek mogelijkheden tot anonimiteit en heimelijkheid. De technologie is gemakkelijk verkrijgbaar, vergt minieme investeringen en attributie is vaak problematisch. Dit vormt een belangrijke uitdaging met betrekking tot het vormen van effectief internationaal beleid, aangezien controle op gemaakte afspraken moeilijk wordt gemaakt.
- *In vrijwel alle internationale discussies over het cyberdomein is er sprake van een scherpe tegenstelling.* Enerzijds zijn er de op het multistakeholder-model en internationaal recht georiënteerde landen, waaronder Nederland, die pleiten voor bescherming van de integriteit van het internet en de toepassing van internationaal recht. Anderzijds zijn er meer staatsgeoriënteerde landen die pleiten voor meer controle van staten en beperkte toepasbaarheid van internationaal recht. Tussen deze kanten van het spectrum bevindt zich een grote groep landen die op basis van hun eigen politiek-economische en sociaal-maatschappelijke belangen nog geen duidelijk keuze heeft gemaakt; de zogenoemde *swing states*. Nederland wil hen er van overtuigen dat zij op basis van deze nationale belangen baat hebben bij een vrij, open en veilig internet.
- *Digitale technologieën verspreiden zich snel in wisselwerking met toegenomen welvaart en groeiende behoefte aan connectiviteit.* Toch is 60 procent van de wereldbevolking nog steeds offline en kan niet deelnemen aan de digitale economie. De digitale kloof blijft daardoor groot en de voordelen van de digitale revolutie worden niet breed gedeeld. De digitale kloof raakt in het bijzonder de ontwikkelingslanden die daardoor maatschappelijke en economische groei mislopen. Onder meer ontbrekende infrastructuur, gebrek aan expertise en gebrek aan politieke prioritering versterken de digitale kloof en zijn daarmee een bedreiging van duurzame ontwikkeling.

2.4 Visie en uitgangspunten

Op basis van de geïdentificeerde internationale belangen, dreigingen en uitdagingen gaat het kabinet uit van de volgende visie:

> *De Nederlandse overheid zet internationaal samen met de private sector, de technische gemeenschap, academici en non-gouvernementele organisaties in op een veilig, vrij en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.*

Net zoals in Nederland is de samenhang tussen groei, veiligheid en vrijheid ook internationaal een dynamische balans die tot stand moet komen in een constante, open en pragmatische dialoog tussen alle stakeholders. Het kabinet gaat daarbij onder meer uit van de volgende uitgangspunten:

1. Het beleid binnen het cyberdomein is gericht op het scheppen van gunstige randvoorwaarden op basis waarvan burgers, bedrijven en overheden hun activiteiten kunnen ontplooien. Vanwege het

grensoverschrijdende karakter van het cyberdomein kunnen randvoorwaarden pas goed worden ingevuld als ze internationaal worden afgestemd.
2. Nederland sluit aan op bestaande internationale structuren, (beleids)instrumenten en samenwerkingsverbanden en versterkt deze waar nodig.
3. Net als nationaal beleid, zal internationaal beleid in het cyberdomein volgens het multistakeholder-overlegmodel en in publiek-private samenwerking worden ontwikkeld en uitgevoerd. Hierbij worden de private sector, de technische gemeenschap, academici en non-gouvernementele organisaties (NGO's) betrokken.
4. Economische en maatschappelijke voordelen van het internet zijn afhankelijk van het betrouwbaar, voorspelbaar, stabiel, en veilig functioneren van de 'publieke kern' van het internet. Deze kern vertoont kenmerken van een internationaal publiek goed dat afzonderlijke soevereine en particuliere belangen overstijgt. Nederland erkent dat de aard en de afhankelijkheid van het cyberdomein vragen om terughoudendheid ten aanzien van activiteiten die aan de publieke kern kunnen raken. De instandhouding en ontwikkeling van de 'publieke kern' dient zoveel mogelijk te worden voorbehouden aan de technische gemeenschap en de statelijke rol zo veel mogelijk op de ondersteuning daarvan.
5. Consistentie tussen binnenlands en buitenlands beleid is van belang. Enerzijds dienen de internationale standpunten van Nederland te volgen uit de nationale praktijk en is het uitgangspunt 'preach what you practice'. Anderzijds leiden nationale maatregelen die afwijken van Nederlandse internationale standpunten en internationale verdragsverplichtingen tot een vermindering van geloofwaardigheid en effectiviteit bij het streven naar internationale ordening. In dat opzicht geldt ook 'practice what you preach' als een uitgangspunt van nationaal beleid. Uiteraard geldt dat Nederland pas gehouden is aan internationale regelgeving als daarover internationaal overeenstemming is bereikt en Nederland de betreffende verplichting is aangegaan.
6. Het grensoverschrijdende karakter van het internet vereist dat uitdagingen en dreigingen die zich hier op het gebied van veiligheid voordoen internationaal aangepakt worden. Aangezien de internationale rechtsorde gebaseerd is op het principe van soevereiniteit kan de nationale overheid de veiligheidsuitdagingen op het internet slechts in beperkte mate eigenstandig ondervangen. Daarvoor is internationale samenwerking volgens een geïntegreerde benadering vereist.

3. Aanpak

Het kabinet benadert de internationale samenwerking op het gebied van cyberbeleid op een integrale wijze. Daarbij worden verschillende werkterreinen onderscheiden. Deze worden hieronder uiteengezet. Tevens worden perspectieven voor verdere beleidsontwikkeling weergegeven.

3.1 Internationale samenwerking, diplomatie en versterking van internationale juridische kaders

Net als in Nederland is effectief internationaal samenwerken op het gebied van cyberbeleid een gezamenlijke inspanning. Dat gebeurt zowel op operationeel vlak tussen uitvoeringsorganisaties als op het beleidsmatige vlak. Hierbij wordt langs de onderstaande sporen gewerkt.

A. Om de Nederlandse internationale en nationale belangen te behartigen bouwt het kabinet aan brede coalities en partnerschappen. Dat gebeurt zowel op bilateraal als op multilateraal vlak in internationale organisaties zoals de Verenigde Naties (VN), de Europese Unie (EU), de Noord-Atlantische Verdragsorganisatie (NAVO), de Raad van Europa, de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) en de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE). Ook de private sector, de technische gemeenschap, de academische wereld en de non-gouvermentele sector worden hierbij betrokken via multistakeholder en publiek-private platforms zoals het *Internet Governance Forum* (IGF), de *Internet Corporation for Assigned Names*

and Numbers (ICANN), het in juli door de EU gelanceerde *Contractual Public-Private Partnership* (cPPP) en Europese *Information Sharing and Analysis Centres* (ISACs).

B. Op deze coalities en partnerschappen is een breed palet aan operationele samenwerking gebaseerd, vooral op het gebied van veiligheid. Dit gebeurt via platforms als het *Forum of Incident Response and Security Teams* (FIRST), de *Task Force Computer Security Incident Response Teams* (TF CSIRT), het *Malware Information Sharing Platform* (MISP) en het Europese CSIRT-netwerk waar nationale partijen als het Nationaal Cyber Security Centrum (NCSC) en het Defensie *Computer Emergency Response Team* (DEFCERT) in deelnemen.

   Binnen de hele cybersecurity-keten en bij de bestrijding van cybercrime, van preventie tot detectie en respons tot opsporing en vervolging, wordt internationaal samengewerkt met inbegrip van wederzijdse rechtshulp in strafzaken. Het merendeel van de betrokken organisaties hebben daarvoor hun eigen netwerken. In geval van grootschalige crises en incidenten kan het reguliere Nederlandse diplomatieke instrumentarium worden ingezet, complementair aan de inzet van reguliere en bestaande crisisstructuren zoals in het kader van de NAVO, de EU *Integrated Political Crisis Response* (ICPR) en het nationaal handboek crisisbesluitvorming onverlet.

C. Nederland zet in op het opbouwen en bevorderen van een internationaal juridisch en normatief kader voor het cyberdomein. Er is sprake van een overheidsbrede inzet in internationale fora waar over internationale standaarden en normen wordt gesproken. Deze variëren van technisch tot beleidsmatig en van vrijwillig tot juridisch bindend. Het gaat daarbij om gebieden zoals internet governance, internationale vrede en veiligheid, de bestrijding van cybercrime en het bewaken van fundamentele rechten online.

Aan deze inspanningen leveren de direct betrokken ministeries als Buitenlandse Zaken (BZ), Economische Zaken (EZ), Veiligheid en Justitie (V&J), Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Defensie (Def) een actieve bijdrage. In het bijzonder zijn overheidsinstanties zoals het Openbaar Ministerie (OM), de politie, de inlichtingen- en veiligheidsdiensten, het Defensie Cyber Commando (DCC) en het NCSC hier bij betrokken.

Bij de *Global Conference on Cyber Space* (GCCS) in 2015 is de Taskforce Cyber gelanceerd die vanuit BZ de diplomatieke inzet in het cyberdomein in goede banen leidt. Daarnaast is er een Speciaal Gezant voor internationaal cyberbeleid die Nederland op internationaal gebied vertegenwoordigt op cybersecurity-gerelateerde zaken. Naast de geïntegreerde aanpak van grensoverschrijdende crises, zet Nederland ook diplomatie in om te komen tot onder meer een normatief kader voor de regulering van cyberoperaties tussen staten. Dit is op lange termijn nodig om tot structurele oplossingen te komen. De ontwikkeling van dit normatieve kader verloopt echter geleidelijk en de uitvoering en naleving hiervan kent beperkingen. Zeker op korte termijn biedt dit niet in alle gevallen een oplossing voor de dreigingen waar Nederland zich mee geconfronteerd ziet. Ontwikkeling van capaciteiten ter verdediging van onze veiligheid is daarom ook van belang.

3.2 Cyber Defence & Security

Nederland stelt de veiligheid van zijn netwerken tegen dreigingen van internationaal opererende criminelen, statelijke en niet-statelijke actoren centraal. Om de nationale veiligheid van Nederland te beschermen tegen dreigingen uit het buitenland ontwikkelt Nederland robuuste capaciteiten. Deze zijn gebaseerd op de doelstellingen van vroegtijdige herkenning, actieve verdediging en, indien noodzakelijk, interventie. Nederland streeft ernaar deze capaciteiten mede in internationaal verband op te bouwen en deze opbouw met inachtneming van de Nederlandse belangen te beïnvloeden. De ruimte voor het uitvoeren van rechtmatige, noodzakelijke en proportionele cyberoperaties door Nederland dient te allen tijde behouden te blijven. Specifiek met betrekking tot de inzet van offensieve

capaciteiten is het uitgangspunt daarbij dat Nederland, net zoals met de inzet van andere geweldsmiddelen, uiterst terughoudend zal zijn en alleen zal optreden als daar een adequate nationale of internationale rechtsgrondslag voor bestaat. Dit is tevens in lijn met NAVO-beleid. Het kabinet richt zich binnen de NAVO ook op het versterken van de afschrikking en de collectieve verdediging door het bondgenootschap. Omdat militaire, inlichtingen-, opsporings- en cybersecurity-capaciteiten in de 21e eeuw onlosmakelijk verbonden zijn door en met netwerken, werkt Nederland zelfstandig en in bondgenootschappelijk verband aan de ontwikkeling van defensieve en offensieve slagkracht voor een groeiend, veilig en geloofwaardig cyber-ecosysteem. Dit gebeurt onder meer via het DCC, NCSC en de inlichtingen- en veiligheidsdiensten.

3.3 Capaciteitsopbouw

Het is van belang de internationale digitale kloof tussen technologisch meer en minder ontwikkelde landen te dichten zodat derde landen kunnen profiteren van de kansen die wereldwijde digitalisering biedt. Capaciteitsopbouw binnen het cyberdomein is dan ook van groot belang. In de conclusies van de Raad van de Europese Unie over Cyber Diplomacy uit 2015 wordt capaciteitsopbouw in derde landen omschreven als een essentiële bouwsteen voor een EU-benadering van cyberdiplomatie waarin mensenrechten, rechtsstaat, veiligheid, groei en ontwikkeling centraal staan. Ook in breder internationaal verband, zoals de *World Summit on the Information Society* (WSIS) en het *UN Group of Governmental Experts* (UNGGE) Rapport 2015, groeit de aandacht voor capaciteitsopbouw. Nederland heeft in het licht van deze ontwikkelingen tijdens de GCCS in 2015 in Den Haag het *Global Forum on Cyber Expertise* (GFCE) gelanceerd. De oprichting van het GFCE heeft internationale capaciteitsopbouw op de terreinen van cybercrime bestrijding, cybersecurity, databescherming en e-governance een belangrijke impuls gegeven. Het GFCE is een pragmatisch, strategisch en flexibel platform voor beleidsmakers, professionals en experts uit verschillende landen, bedrijven en internationale organisaties. Binnen het GFCE wordt samengewerkt met verschillende beleidsdepartementen, academici, NGO's en de technische gemeenschap. Nederland moedigt andere staten aan om de visie van een vrij, open en veilig internet te omarmen en biedt capaciteit om deze visie te implementeren.

Het instrument capaciteitsopbouw dient zowel korte als lange termijndoelstellingen die belangrijk zijn voor Nederland. Het doel is om het kennis- en expertiseniveau van derde landen naar een zo hoog mogelijk niveau te brengen om de zwakke schakels in de wereldwijde internetinfrastructuur te versterken. Op de korte termijn helpt capaciteitsopbouw bij het verbeteren van de digitale weerbaarheid van partnerlanden en ondersteunt het hun vermogen om te profiteren van de economische voordelen van de digitale economie. Op langere 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.

3.4 Perspectieven voor verdere beleidsontwikkeling

Om optimaal in te spelen op de kansen en uitdagingen die de technologische ontwikkelingen ons bieden is een geïntegreerde internationale benadering van het cyberdomein belangrijk. Hiervoor zal het kabinet de bestaande internationale samenwerking en diplomatie versterken. Zo zal het kabinet een cyberdiplomatennetwerk voor het Nederlandse cyberbeleid activeren, beginnend op een aantal belangrijke ambassades. Dit zal binnen de bestaande begroting van BZ worden opgevangen.

Cyberdiplomaten werken vanuit ambassades en vertegenwoordigingen aan een open, vrij en veilig cyberdomein. Ze fungeren onder meer als liaison voor andere overheden en internationale organisaties, informeren over trends en ontwikkelingen en ondersteunen inhoudelijk bij strategische prioriteiten. Hiervoor werken ze samen met de V&J, EZ en Defensie attaches, het bedrijfsleven, academici en NGO's. De komende periode zal worden bezien hoe het cyberdiplomatennetwerk verder geactiveerd kan worden.

Daarnaast zal worden bezien hoe de samenwerking in EU verband, die Nederland als Voorzitter van de Raad van de EU in 2016 in belangrijke mate op de kaart heeft gezet, op duurzame wijze verder kan worden versterkt. Daartoe bieden onder andere de *Global Strategy for the European Union's Foreign and Security Strategy*, de *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace,* de Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIB) en de Europese Commissie mededeling inzake *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry* aanknopingspunten. Versterking van de weerbaarheid van de EU en zijn lidstaten waar het kritieke infrastructuur betreft en de versterking van een raamwerk voor cybercrisis management staan voorop. Het ligt verder voor de hand cyberbeleid verder te integreren in het gemeenschappelijk buitenlands en veiligheidsbeleid en te bezien hoe de samenwerking met partners zoals de VS, Canada, NAVO en de OVSE kan worden verstevigd. Ook in EU-verband dient publiek-private samenwerking en de multistakeholder benadering waar van toepassing de voorkeur te hebben. Zowel EDEO en de EU-vertegenwoordigingen in derde landen als betrokken onderdelen van de Europese Commissie kunnen bijdragen aan een effectief internationaal EU-cyberbeleid.

4. Beleidsprioriteiten van een internationale cyberstrategie

De visie van de internationale cyberstrategie is uitgewerkt in de volgende beleidsprioriteiten:
- Economische groei en duurzame ontwikkeling van het internet;
- Effectieve internet governance;
- Verdere versterking cybersecurity;
- Effectieve bestrijding cybercrime;
- Internationale vrede, veiligheid en stabiliteit;
- Rechten en internetvrijheid.

Hieronder worden de beleidsprioriteiten uitgewerkt.

4.1 Economische groei en duurzame ontwikkeling van het internet

Ruim een derde van onze economische groei komt van digitale bedrijvigheid. Als digitale toegangspoort tot Europa heeft Nederland de ambitie zijn positie als een *safe place to do business* verder te versterken. Hiervoor zijn robuuste cybersecurity en respect voor rechten en vrijheden in het cyberdomein belangrijke randvoorwaarden.

Voor het tegengaan van *abuse online* en *Distributed Denial of Service* (DDoS) aanvallen wordt in een aantal internationale multistakeholder en multilaterale fora gesproken over internet governance, *open source* standaarden en over *private best practices*. Nederland draagt hier actief aan bij. Dit geldt ook voor de discussie en besluitvorming binnen de EU over zaken als ICT standaardisatie, stimulering van de cybersecurity industrie, een gelijk speelveld en certificering van producten.

Daarnaast zal de overheid door middel van het multistakeholder-overlegmodel kader- en normstellend moeten optreden waar nodig. De relatie tussen de overheid en bedrijven is dynamisch. Bedrijven zijn belangrijke partners bij het waarborgen van publieke belangen als privacy, veiligheid en vrijheid in het cyberdomein. Anderzijds kunnen bedrijven, bijvoorbeeld door hun wereldwijde dominante marktpositie, ook negatieve invloed hebben. Gezien hun sleutelrol in het cyberdomein is het belangrijk deze bedrijven bij het debat te betrekken.

De centrale vraag is op nationaal niveau: hoe zorgen we er gezamenlijk voor dat het internet qua standaarden up-to-date blijft en niet achteropraakt? Gezamenlijk optrekken creëert meer urgentie en draagt bij aan een bredere verspreiding van kennis. Voorbeeld daarvan is het Platform Internetstandaarden. In dit platform nemen partijen plaats als Stichting Internetdomein Nederland

(SIDN), *Réseaux IP Européens Network Coordination Centre* (RIPE NCC), Internet Society Nederland (ISOC) en de overheid.

Met betrekking tot gevoelige onderwerpen is heldere en toekomstbestendige regelgeving essentieel om het internationale bedrijfsleven investeringszekerheid en een aantrekkelijk vestigingsklimaat te bieden. Hierbij valt te denken aan onderwerpen als cybersecurity, privacy, encryptie, data-bescherming en –opslag (al dan niet door de overheid), gebruik van open data, netneutraliteit, digitale authenticatie en identificatie en aansprakelijkheid voor producten of diensten.

Om de Nederlandse kenniseconomie en innovatiepositie te beschermen zet het kabinet zich ook in voor het tegengaan van digitale economische spionage. Op nationaal niveau verrichten de AIVD en de MIVD onderzoek naar de dreiging. De bevindingen worden waar mogelijk met de slachtoffers en belanghebbenden gedeeld. Op internationaal niveau zal de bestaande internationale samenwerking en diplomatie worden versterkt.

4.2 Effectieve internet governance

De governance van het internet is uniek. Geen enkele private partij, organisatie of overheid oefent als enige gezag uit op het internet of kan de werking van het internet substantieel beïnvloeden. Het kabinet zet in op waarborging van deze unieke en effectieve methode van internet governance. Het internet wordt werkend gehouden door diverse actoren: onderzoeksinstituten, standaardisatie- en technische organisaties, het bedrijfsleven, het maatschappelijk middenveld, gebruikersorganisaties en overheden.

Dit multistakeholder-overlegmodel staat ook aan de basis van de grote mate van zelfregulering en zelforganisatie binnen het internet. Hierin staat 'bottom-up' participatie, openheid en non-discriminatie centraal. Om de vrijheid, openheid en veiligheid van het internet te waarborgen is het van belang dat internet governance bij de multistakeholder-internetgemeenschap blijft. Overheden nemen daaraan actief deel, maar belemmeren de processen niet door unilaterale of multilaterale inmenging.

De verlenging van het mandaat van het mondiale Internet Governance Forum (IGF) met tien jaar krachtens Resolutie 70/125 van de Algemene Vergadering van de VN van 16 december 2015 was dan ook een belangrijke mijlpaal, waarmee steun aan het multistakeholder-overlegmodel van internet governance alom werd herbevestigd. Tegelijkertijd werd met deze resolutie opgeroepen meer haast te maken met de implementatie van de aanbevelingen van een VN-werkgroep uit 2012 om het IGF te verbeteren. Het gaat daarbij onder andere om ontwikkelingslanden meer te betrekken bij het IGF, maar ook om de resultaten van dit mondiale overlegplatform tastbaarder en zichtbaarder te maken. Nederland werkt daaraan actief mee.

De recente, door Nederland gesteunde, *Internet Assigned Numbers Authority* (IANA) transitie, waarbij ICANN het volledige toezicht verwierf over het beheer van het domeinnamensysteem (DNS), was een belangrijke stap voor internet governance. De opgave voor de komende jaren is om de transparantie en de verantwoordingsstructuur van ICANN verbeteren en ervoor te zorgen dat ICANN verder internationaliseert. Het kabinet zet daarom in op een actievere rol voor het comité van nationale overheden binnen ICANN, de *Governmental Advisory Committee* (GAC), die wel een adviserende rol zal behouden.

Nederland heeft zijn positie binnen het internet governance debat gemarkeerd door met ruim honderd andere landen, het bedrijfsleven, de technische internetgemeenschap en de belangrijkste internet governance organisaties de slotverklaring van de NETmundial-conferentie 2014 te onderschrijven. In deze verklaring zijn de principes vastgelegd voor internet governance, waaronder vrijheid op het

internet, respect voor mensenrechten en een verdere verankering van het multistakeholder-overlegmodel.

Gezien de wereldwijde publieke belangen die verbonden zijn aan het internet zet het kabinet daarnaast in op de erkenning van de kern van het internet als *international public good*. Nederland erkent dat de aard en de afhankelijkheid van het digitale domein vragen om terughoudendheid ten aanzien van activiteiten die aan de 'publieke kern' kunnen raken. Nederland werkt aan het ontwikkelen en geaccepteerd krijgen van internationale gedragsregels en normen en heeft hiervoor een initiatiefvoorstel ingediend bij de *United Nations Group of Governmental Experts* (UN GGE*) on Developments in the Field of Information and Telecommunications in the Context of International Security*.

4.3 Verdere versterking cybersecurity

De samenhang tussen veiligheid, vrijheid en maatschappelijke groei is een dynamische balans. Een open en vrij cyberdomein kan niet worden gegarandeerd zonder veiligheid.
Het kabinet zet zich daarom zowel bilateraal, regionaal als multilateraal actief in voor de bevordering en versterking van cybersecurity. Zo worden Nederland en het cyberdomein veilig gemaakt.

Zoals het CSBN jaarlijks inzichtelijk maakt is de cyberdreiging van staten, criminelen en niet-statelijke actoren gericht op Nederlandse politieke, economische en maatschappelijke belangen reëel en toenemend. Het kabinet werkt daarom al geruime tijd aan het versterken van de veiligheid in het cyberdomein, zoals beschreven in de strategische doelstellingen van de NCSS 2. Deze doelstellingen gelden evenzeer voor het internationale cyberdomein. Hiertoe behoort het versterken van de weerbaarheid tegen cyberaanvallen en de bescherming van vitale belangen in het cyberdomein, publiek-private samenwerking, detectie, respons en bewustwording en onderwijs. Nederland geeft mede richting op internationaal niveau, aangezien het cyberdomein geen grenzen kent en veiligheid alleen kan bestaan door een gezamenlijke inzet op de zwakste schakels.

4.3.1 Versterking van de Europese digitale veiligheid

Het kabinet zet zich internationaal in voor een integrale aanpak van cybersecurity. Dit gebeurt door middel van cybersecuritystrategieën op nationaal niveau, technologie neutrale Europese wetgeving die up-to-date is en het stimuleren van privaat-publieke samenwerking. Daarbij gaat in het bijzonder aandacht uit naar vitale sectoren en infrastructuren en het bevorderen van een gelijk speelveld. Deze inzet vindt vooral binnen de Europese Unie plaats maar ook in toenemende mate daarbuiten in bilaterale en multilaterale verbanden. De inwerkingtreding van de Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIB) is een belangrijke stap waarvan Nederland één van de voortrekkers is.

De 'Samenwerkingsgroep' is opgericht met als taak de strategische samenwerking en de uitwisseling van informatie tussen EU 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 inzet van het kabinet is erop gericht om via deze samenwerkingsgroep op strategisch niveau richting te geven aan de verbetering van de digitale veiligheid in Europees verband. De recente Commissie-Mededeling over de versterking van het cyberbeveiligingssysteem en cyberbeveiligings-branche is een belangrijke volgende mijlpaal voor Europese samenwerking. Ook op strategisch en politiek niveau is Nederland actief ten behoeve van onder andere bewustzijnsvergroting, wederzijds begrip en verantwoordelijkheidstoedeling.

4.3.2 Operationele inzet en samenwerking op cybersecurity
Nederland werkt ook op internationaal niveau operationeel intensief samen. De operationele samenwerking draagt bij aan robuuste informatie- en kennisdeling, incidentmanagement, weerbaarheid en herstelcapaciteiten. Dit vindt veelal plaats via vertrouwde netwerken. De samenwerking vindt plaats tussen *Computer Security Incident Response Teams* (CSIRTs), ook wel CERTs, maar ook door Nederlandse inlichtingen- en veiligheidsdiensten in bilaterale en multilaterale verbanden. Nederland speelt in deze internationale arena een prominente rol. De operationele samenwerking komt ook weer ten goede aan de veiligheid, vrijheid en maatschappelijke groei van zowel het private als publieke domein. Ten behoeve van het bevorderen van het vertrouwen en operationele samenwerking tussen CSIRTs binnen de EU is met inwerkingtreding van de NIB-richtlijn een CSIRT-netwerk opgericht. Nederland spant zich in het bijzonder in om dit netwerk te operationaliseren en tot een succes te maken.

4.3.3 Stimuleren van cybersecurityonderzoek
De Nationale Cybersecurity Research Agenda (NCSRA) dient als basis voor het korte en lange termijn onderzoek in nationaal en internationaal verband. De thema's sluiten aan bij de NCSS 2 met als doel cybersecuritykennis en -kunde te vergroten en te investeren in ICT-innovatie om onze cybersecuritydoelstellingen te behalen.
Ook wordt in dit kader samenwerking in cybersecurityonderzoek uitgevoerd tussen de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en het Amerikaanse *Department of Homeland Security* (DHS).

4.4 Effectieve bestrijding cybercrime
Cybercriminelen werken steeds geavanceerder en zijn beter georganiseerd waardoor de schade van cybercrime toeneemt. Deze ontwikkelingen worden versterkt door de relatief lage kosten en risico's voor de plegers van cybercriminaliteit of -spionage. De kosten en risico's voor conventionele fysieke vormen van criminaliteit zijn vaak hoger en de opbrengsten lager.

Het is de taak van de overheid de rechtsstaat te handhaven, ook in het cyberdomein. Het gebruikelijke systeem van internationale rechtshulp is echter zeer traag in vergelijking met de snelle ontwijkingsmogelijkheden die criminelen benutten. Dit gebeurt bijvoorbeeld door hun activiteiten via diverse landen te geleiden en door hun gegevens snel tussen diverse landen te verplaatsen. Daarbij worden vaak landen gekozen waar de wetgeving of de capaciteiten ontoereikend zijn om cybercriminelen aan te pakken. Het cyberdomein dreigt daarmee voor technisch vaardige criminelen een vrijplaats te worden voor het plegen van strafbare feiten. Om internationale opsporing in het cyberdomein te bevorderen zet Nederland in op de intensivering van internationale samenwerking en het versterken van de internationale juridische kaders. Nederland heeft deze onderwerpen geagendeerd op de GCCS 2015 en tijdens het EU-voorzitterschap. Ook de versterking van capaciteiten en juridische kaders in andere landen is van belang. Dit wordt ondersteund met capaciteitsopbouwprojecten die in het kader van het Cybercrimeverdrag onder coördinatie van de Raad van Europa worden uitgevoerd.

4.4.1 Internationale samenwerking voor opsporing in het cyberdomein
De bestrijding van cybercriminaliteit stelt nieuwe eisen aan vooral de handelingssnelheid en informatie-uitwisseling tussen politie, justitie en private partijen. De JBZ-raad heeft in juni 2016 raadsconclusies aangenomen over de start van een Europees netwerk van openbaar aanklagers, met ondersteuning van Eurojust, en over mogelijkheden voor een gezamenlijk EU platform voor het uitwisselen van informatie over elektronisch bewijs. Ook zijn raadsconclusies aangenomen over jurisdictie in het cyberdomein, waar het versterken van de rechtshulpprocedures deel van uit maakte. Daarnaast heeft het *Standing Committe on Internal Security* (COSI) op basis van ervaringen uit de praktijk concrete aanbevelingen aangenomen voor versterking van de operationele samenwerking.

Ook heeft Nederland bijgedragen aan de ontwikkeling van het *European Cyber Crime Centre* bij Europol en ondersteunt Nederland het *INTERPOL Global Complex for Innovation* (IGCI) in Singapore. Het IGCI is onder meer opgericht om de wereldwijde internationale samenwerking in cybercrimezaken beter te kunnen ondersteunen.

4.4.2 Versteviging van de mogelijkheden voor de opsporing in het cyberdomein
De ontwikkelingen in het digitale domein vergen een heroverweging van de internationale juridische kaders. Zeker 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. Tijdens het Nederlandse EU-voorzitterschap heeft de JBZ-raad raadsconclusies aangenomen waarin de Europese Commissie is verzocht voorstellen te ontwikkelingen voor een betere samenwerking met private partners in andere landen. Daarnaast is de Commissie verzocht uit te werken welke aanknopingspunten er mogelijk zijn voor handhavingsjurisdictie anders dan territorialiteit, en of er opsporingsbevoegdheden zijn die onafhankelijk van territoriale grenzen gebruikt zouden kunnen worden.
Nederland draagt bovendien het belang uit van bredere ratificering van het Cybercrimeverdrag van de Raad van Europa.Tevens is Nederland voorstander van de ontwikkeling van een Additioneel Protocol bij het Cybercrimeverdrag, waarin de mogelijkheden voor de internationale opsporing van cybercrime verder worden uitgebreid.

4.5 Internationale vrede, veiligheid en stabiliteit
In het cyberdomein lijkt een situatie te ontstaan van wantrouwen en gevaar op escalatie en miscalculatie. Defensieve maatregelen genomen door de ene staat kunnen mogelijk worden geïnterpreteerd als een bedreiging door andere staten. Dit kan zorgen voor internationale instabiliteit en brengt het risico van een mogelijke wapenwedloop met zich mee. Om dit beheersbaar te houden, om de geïdentificeerde internationale veiligheidsbelangen te verdedigen en om de dreiging van statelijke actoren het hoofd te bieden wordt de in de NCSS 2 reeds geïdentificeerde 3D aanpak van defence, diplomacy en development verder ontwikkeld. Het uitgangspunt daarbij is dat cyberoperaties voor statelijke actoren uiteindelijk slechts een middel zijn om hun bredere geopolitieke en economische doelstellingen te bereiken. Naast het verhogen van de nationale en internationale digitale weerbaarheid is daarom ook het beïnvloeden van het gedrag van statelijke actoren een belangrijk doel van deze beleidsprioriteit.

4.5.1 Militaire capaciteiten
Omdat militaire capaciteiten in de 21^{e} eeuw onlosmakelijk verbonden zijn door en met netwerken werkt Nederland met vertrouwde partners aan de ontwikkeling van defensieve en offensieve slagkracht voor een groeiend, veilig en geloofwaardig cyber-ecosysteem. Het kabinet stelt de veiligheid van zijn netwerken tegen internationaal opererend statelijke en niet-statelijke actoren voorop. Met inachtneming van nationale wetgeving en internationale afspraken wordt er ingezet op de combinatie van weerbare nationale netwerken en de ontwikkeling van internationaal geloofwaardige interventiecapaciteiten. Deze maatregelen zijn gericht op afschrikking van eventuele vijandige of criminele actoren.

Nederland hecht binnen de eigen grenzen aan een cultuur en ecosysteem waarbij publieke en private partijen gezamenlijk cybersecurity nastreven. Adequate respons en een tijdig herstel van de integriteit, beschikbaarheid en vertrouwelijkheid staan hierbij centraal. Internationaal streeft Nederland, ook in bondgenootschappelijk verband, naar robuuste en geloofwaardige capaciteiten, gebaseerd op de principes van vroegtijdige herkenning, actieve verdediging en indien noodzakelijk interventie.

Ter bescherming van de Nederlandse internationale en nationale veiligheidsbelangen speelt Nederland daarom ook een leidende rol in het opbouwen van een sterke collectieve verdediging van de NAVO in het cyberdomein. Op de top in Warschau in 2016 heeft de NAVO cyberspace als een apart domein van operaties erkend, zodat cyberaspecten voortaan in het volledige operationele proces kunnen worden meegenomen. Naast het belang van een veilig operationeel proces, is de cyberverdediging van de alliantie zo sterk als de zwakste schakel. Met de Cyber Defence Pledge hebben alle bondgenoten een politiek statement uitgebracht waarmee zij zich committeren aan het verder versterken van nationale cyber verdediging van nationale netwerken en infrastructuur.

4.5.2 Internationaal recht, gedragsnormen en vertrouwenwekkende maatregelen
Het kabinet zet op middellange termijn in op het bewerkstelligen van een internationaal normatief kader voor de regulering van cyberoperaties tussen staten. Het bestaande internationaal recht is daarvan de belangrijkste component. Het verhelderen van de toepassing van het internationaal recht op cyberoperaties is de belangrijkste Nederlandse prioriteit op dit gebied. Als klein land heeft Nederland belang bij een goed functionerende internationale rechtsorde die zorgt voor een mate van voorspelbaarheid, stabiliteit en conflictpreventie. In het kader hiervan ondersteunt Nederland door middel van het 'The Hague Process' aan de hand van de Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations meer inclusieve en meer gedetailleerde discussie over de toepassing van het internationaal recht op cyberoperaties. Het kabinet zet daarnaast in op internationale afspraken over niet-bindende, vrijwillige gedragsnormen voor staten en vertrouwenwekkende maatregelen. Nederland draagt zo bij aan de ontwikkeling van een internationale veiligheidsarchitectuur voor het cyberdomein, waarmee het veiligheidsdilemma beter beheersbaar wordt. Deze veiligheidsarchitectuur leidt tot meer stabiliteit en het verkleinen van het risico van escalatie, miscommunicatie en miscalculatie. Onder meer zal Nederland hiertoe de Global Commission on the Stability of Cyberspace lanceren, die als multistakeholder-platform een mondiale discussie over nieuwe vrijwillige gedragsnormen in het cyberdomein zal faciliteren.

4.5.3 Transparantie offensieve militaire cybercapaciteiten
Het kabinet is transparant over de Nederlandse ambitie om militaire cybercapaciteiten te ontwikkelen. Op dat gebied pleit Nederland internationaal ook voor meer transparantie van andere landen. Daarbij gaat het niet om de aard van die capaciteiten, maar om transparantie over de doelen waar die capaciteiten toe dienen, het juridische kader waaronder zij worden ingezet en de politieke controle en het democratisch toezicht op de inzet daarvan. Transparantie op dit vlak is 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.

4.5.4 Exportcontrole en EU Dual-Use verordening
Ten behoeve van het waarborgen van internationale veiligheid en mensenrechten zet het kabinet in op een verbod op of het verplicht stellen van een exportvergunning voor specifieke hardware, software en technologie. Wat hieronder valt is vastgesteld in de Wassenaar Arrangement lijsten van te controleren goederen. Deze lijsten worden integraal overgenomen in Europese wetgeving, de Dual-Use Verordening, waarmee het toezicht op handel in goederen voor tweeërlei gebruik is vastgelegd. Daarbij gaat het onder andere om intrusion software die door autoritaire regimes gebruikt kan worden voor het inperken van burgerrechten.

Het kabinet is voorstander van uitbreiding van de al bestaande controle op apparatuur voor smart surveillance met een mensenrechten-grondslag. Daarentegen staat het kabinet uiterst kritisch tegenover het voorstel van de Europese Commissie om als herziening van de Dual-Use Verordening een nieuwe categorie goederen aan de controlelijst toe te voegen. Deze aanpak kan leiden tot

verdubbelde regelgeving of juist tegenstrijdigheden. Bovendien verstoort het zo het gelijke speelveld op mondiaal niveau ten nadele van de Europese industrie, omdat de autonome controlelijst alleen geldt voor de EU.

4.5.5 Capaciteitsopbouw

Om kansen die digitalisering onze internationale gemeenschap en economie biedt volop te benutten en dreigingen het hoofd te kunnen bieden zet het kabinet in op capaciteitsopbouw. Het doel daarbij is om wereldwijd, in het bijzonder binnen Europa, een basisniveau van cybersecurity te bevorderen. In dit kader deelt Nederland kennis, best practices en training op het terrein van cybersecurity. Zo wordt het belang Coordinated Vulnerability Disclosure (CVD) actief uitgedragen in Europese en internationale platforms, waaronder de EU en het GFCE. Ook wordt ingezet op verdere ontwikkeling van CSIRT bekwaamheid, ofwel CSIRT Maturity. Ook draagt Nederland onder andere bij aan het vergroten van het vermogen van verschillende actoren op het gebied van veiligheid en mensenrechten online door middel van capaciteitsopbouw. Nederland draagt bij aan processen en toepassingen van digitalisering op landenniveau en op maatschappelijk niveau steunt Nederland projecten die digitale technologieën inzetten als katalysator voor duurzame ontwikkeling. Op lange termijn dragen de inspanningen op capaciteitsopbouw bij aan het ontwikkelen van strategische allianties gericht op een vrij, open en veilig cyberdomein.

4.6 Rechten en internetvrijheid

4.6.1 Fundamentele rechten en vrijheden online

Om fundamentele rechten en vrijheden internationaal effectief te bestendigen en uit te dragen, zet het kabinet in op een mensenrechten inclusief internationaal cyberbeleid. De naleving van mensenrechten staat aan de basis staan van een open, vrije en veilige samenleving. Bescherming van persoonsgegevens, privacy, het verbod van discriminatie, de vrijheid van meningsuiting, vrije informatievergaring, het recht op vereniging en vergadering staan onder toenemende druk door overheden. Zij legitimeren disproportioneel ingrijpen met een verwijzing naar het nationale veiligheidsbelang. Nederland beschouwt veiligheid en vrijheid niet als tegengestelde maar als complementaire belangen: een veilige samenleving is een samenleving waarin de fundamentele rechten en vrijheden van het individu beschermd worden. Het kabinet draagt deze mensenrechten inclusieve visie internationaal uit om dialoog hierover te bestendigen.
Nederland draagt in internationale fora en multistakeholder platforms actief bij aan verdere erkenning en waarborging van fundamentele rechten online. Deze erkenning is van belang om negatieve trends die internetvrijheid in steeds meer landen in de verdrukking brengen te keren. Voor het keren van dergelijke trends is internationale samenwerking met alle belanghebbenden van essentieel belang. Het is belangrijk dat landen leren van elkaars *best practices* en dat deze actief worden delen.

Betere diplomatieke coördinatie is van groot belang bij het bewaken van het open en vrije karakter van het Internet in een tijd waarin steeds meer staten trachten een 'nationaal' Internet te creëren. Nederland wil zich actief inzetten voor het betrekken van bedrijven, non-gouvernementele organisaties, de technische en academische gemeenschap.

4.6.2 Het recht op bescherming van persoonsgegevens en het recht op privacy

Om bescherming en erkenning van het recht op bescherming van persoonsgegevens en het recht op privacy te realiseren zet het kabinet in op ondersteuning van initiatieven in verschillende multilaterale fora. Het is van groot belang dat het recht op bescherming van persoonsgegevens en de 'eerbiediging van de persoonlijke levenssfeer' ook wordt beschermd en erkend in de digitale context. Daarvoor zal Nederland blijven zoeken naar coalities met gelijkgestemde landen op dit thema.

Het kabinet heeft begin 2016 het kabinetsstandpunt encryptie gepresenteerd. Het kabinet heeft als taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen. Het kabinet

onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie. Daarnaast zijn overheden, bedrijven en burgers gebaat bij maximale veiligheid van de digitale systemen. Het kabinet onderschrijft het belang van sterke encryptie voor de veiligheid op internet ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven en voor de Nederlandse economie. Tegelijkertijd spelen ook veiligheidsoverwegingen een belangrijke rol. Het kabinet is van mening dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. In het kabinetsstandpunt is benadrukt dat Nederland deze conclusie en de afwegingen die daaraan ten grondslag liggen in de internationale context zal uitdragen.

Om vertrouwen in dataprotectie en privacybescherming te garanderen zet het kabinet in op internationale standaardisering en rechtszekerheid rondom dataoverdracht. Internationale juridische kaders zijn nodig wanneer er gegevensuitwisseling plaatsvindt met landen die lagere standaarden hanteren dan de EU. Internationale standaardisering helpt om een internationaal *level playing field* voor bedrijven te bewerkstelligen, maar de laagste gemene deler moet daarbij niet het uitgangspunt zijn. Uiteindelijk is goede gegevensbescherming in het belang van individu, overheid én bedrijfsleven.