Bijlage: Voortgangsrapportage NCSA

In deze bijlage is een overzicht opgenomen van de voortgang per ambitie van de Nederlandse Cybersecurity Agenda (NCSA). De rapportage bestaat uit een tabel met een overzicht op hoofdlijnen per ambitie, en een schriftelijke uitgeschreven toelichting. Er is een afkortingenlijst opgenomen aan het einde van deze bijlage.

1. Digitale slagkracht op orde

Terugblik	- De personele capaciteit voor detectie en respons bij het NCSC, DCSC en de inlichtingen- en veiligheidsdiensten is verder uitgebreid. - Ook de personele capaciteit van het DCC is gegroeid. - Het afgelopen jaar zijn weer meer rijksoverheidsorganisaties en vitale aanbieders aangesloten op het Nationaal Detectie Netwerk. - Er zijn inmiddels bij ministeriële regeling krachtens de Wbni vier computercrisisteams aangewezen waaraan het NCSC gelet daarop ook bepaalde vertrouwelijke informatie kan verstrekken, namelijk Z-CERT, IBD, SURFcert en CERT-WM. - Cyberweerbaarheidscentrum Brainport, Abuse Information Exchange en NBIP zijn krachtens de Wbni aangewezen als organisatie die objectief kenbaar tot taak heeft om andere organisaties over digitale dreigingen te informeren (OKTT), met als gevolg dat ook zij van het NCSC bepaalde specifieke informatie kunnen ontvangen. - Er wordt nauw samengewerkt tussen Z-CERT, VWS, het NCSC, de NCTV en de inlichtingen- en veiligheidsdiensten tijdens de COVID-crisis. - Om de slagkracht van (semi-)publieke computercrisisteams binnen Nederland te versterken is een Nationaal Respons Netwerk-convenant vastgesteld. - Het aantal cybersecuritysamenwerkingsverbanden dat ondersteund wordt door het DTC is uitgebreid. - NCSC en DTC hebben een samenwerkingsconvenant vastgesteld. - Het CSIRT DSP is volledig operationeel en heeft in meerdere instanties digitale dienstverleners benaderd met advies en bijbehorend handelingsperspectief n.a.v. kwetsbaarheden. - Nationaal Crisisplan Digitaal is geactualiseerd en in februari 2020 naar de Tweede Kamer verzonden.
Vooruitblik	- De personele capaciteit bij het NCSC, DCSC, DCC en de inlichtingen- en veiligheidsdiensten wordt verder vergroot. - De actualisatie van het Nationaal Crisisplan Digitaal wordt voor het einde van 2020 ter hand genomen. - DTC wordt een vast organisatieonderdeel van het ministerie van EZK. - Het DTC vergroot dit jaar het aantal cybersecuritysamenwerkingsverbanden naar minstens 30. - Het DTC levert deze zomer informatiepakketten voor brancheorganisaties én gemeentes op. - Momenteel wordt samengewerkt door EZK en JenV aan het voldoen van het DTC aan de wettelijke voorwaarden waardoor het DTC aangewezen kan worden als zogenaamde OKTT. - De komende periode wordt onderzocht of er nog meer OKTTs aangewezen zullen worden. De informatie-uitwisseling tussen het NCSC enerzijds en computercrisisteams en OKTT's anderzijds wordt nader uitgewerkt om zo snel en efficiënt mogelijk dreigings- en risico-informatie te kunnen delen. - BZK kent de provincies een subsidie toe voor onderzoek naar en mogelijk opzet

	van een provinciaal informatieknooppunt cybersecurity in 2020. - Het operationele samenwerkingsplatform om informatie met handelingsperspectief uit te kunnen wisselen zal in 2020 operationeel zijn.[1] - De publicatie van de Defensievisie (eerder Defensienota genoemd) is gepland voor het najaar 2020. Deze visie laat zien welke rol Defensie in de toekomst moet kunnen vervullen in onder andere het digitale domein. - De verkenning naar strafbaarstelling van spionage, waaronder in het digitale domein, zal worden meenomen naar de volgende kabinetsperiode.

De digitale dreiging die uitgaat van statelijke actoren en criminelen is onverminderd groot. Spionage en (voorbereidingen van) sabotage door statelijke actoren vormen een groot risico voor de nationale veiligheid, zo blijkt uit het Cybersecuritybeeld Nederland (CSBN 2020). Het kabinet blijft daarom investeren in de digitale slagkracht van Nederland, om de digitale weerbaarheid te vergroten. Een belangrijke stap in het verhogen van de digitale weerbaarheid is het verbeteren van het stelsel van informatiedeling over digitale dreigingen (zie hiervoor ook ambitie 4).

Het afgelopen jaar is op diverse vlakken geïnvesteerd in deze verbetering. Zo heeft het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden verder vorm gekregen door het aanwijzen van een viertal sectorale computercrisisteams en drie organisaties die objectief kenbaar tot taak (OKTT) hebben om andere organisaties of het publiek daarover te informeren, respectievelijk de Informatiebeveiligingsdienst (IBD), CERT Watermanagement, SURFcert en Z-CERT alsmede de Nationale Beheersorganisatie Internet Providers (NBIP), Abuse Information Exchange en Cyberweerbaarheidscentrum Brainport. Door deze aanwijzing wordt voor het NCSC een grondslag gecreëerd om persoonsgegevens in zogenaamde restinformatie over digitale dreigingen met deze samenwerkingsverbanden delen. Eind 2019 waren er twintig samenwerkingsverbanden van bedrijven aangesloten bij het Digital Trust Center (DTC). Deze samenwerkingsverbanden zijn sectoraal of regionaal georganiseerd. In november 2019 is ook het digitale platform van het DTC live gegaan. Ook is geïnvesteerd in bestendiging en uitbreiding van de samenwerking tussen het NCSC en het DTC. Het CSIRT DSP (Computer Security Incident Response Team voor digitale dienstverleners) is sinds 1 januari 2019 op volle sterkte en volledig operationeel en heeft bij geconstateerde kwetsbaarheden diverse digitale dienstverleners actief benaderd met advies en bijbehorend handelingsperspectief. Ook wordt er voortdurend geïnvesteerd in samenwerking tussen verschillende overheidslagen, om zo de digitale slagkracht te versterken. Zo is in 2019 verkend wat de status is van de CERT/SOC-taken van provincies, gemeenten en waterschappen. Op basis hiervan zijn de provincies subsidie toegekend voor het opzetten van een eigen cybersecuritysamenwerkingsverband in 2020.

Met de investeringen van dit kabinet is het cybersecurity-gerelateerde budget van de AIVD en MIVD structureel uitgebreid. Deze investeringen dragen bij aan het onderkennen en onderzoeken van-, en vervolgens informeren en adviseren over hoogwaardige digitale dreigingen die uitgaan van statelijke actoren. De geplande versterking van de cybersecurity-capaciteit van de AIVD en MIVD in 2019 is in behoorlijke mate gerealiseerd, en zal tot 2021 doorlopen. Positief effect hiervan in 2019 is onder meer geweest een versterking van het relatienetwerk en de cybersecurity-dienstverlening van de AIVD en MIVD richting publieke, vitale en private organisaties.

Defensie heeft in het afgelopen jaar geïnvesteerd in de uitbreiding van de personele capaciteit en de aanschaf van nieuwe hard- en software binnen de gehele cyberketen. Het Defensie Cyber Security Centrum (DCSC) heeft meer sensoren in gebruik genomen om cyberdreigingen te kunnen detecteren, via het nieuwe *threat intel platform* vervolgens interdepartementaal te kunnen delen en waarop vervolgens met een *cyber rapid response team* kan worden gereageerd. De MIVD heeft haar capaciteit uitgebreid om o.a. met monitoring en analyse bij te kunnen dragen aan attributie.

[1] Het convenant voor dit samenwerkingsplatform is op 15 juni 2020 verschenen in de Staatscourant 2020, 30702.

Tenslotte heeft het Defensie Cyber Commando (DCC) meer personeel aangetrokken om ook het militaire vermogen in het digitale domein te vergroten en ondersteuning te kunnen bieden aan operationele inzet.

Het Nationaal Crisisplan Digitaal is herzien en is in februari 2020 aan uw Kamer aangeboden.[2]

Vooruitblik
De komende periode wordt het landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden verder uitgebouwd. Hierbij wordt voortdurend gekeken naar de meest effectieve en efficiënte manier om binnen de geldende wettelijke kaders onderling informatie te delen binnen dit stelsel. Ook zal binnen de overheid, zoals hierboven al kort werd geschetst, doorgegaan worden met het verbeteren van de samenwerking om zo de digitale slagkracht te vergroten. Zo werken de NCTV, het NCSC, de AIVD, MIVD, Nationale Politie en het Openbaar Ministerie samen aan een platform om de operationele samenwerking te versterken, onder andere voor het verbeteren en versnellen van de analyse van cyberincidenten en –dreigingen. Dit platform wordt in 2020 operationeel.

Gegeven het belang van veilig digitaal ondernemen voor ondernemend Nederland is besloten dat het DTC na de programmaperiode 2018-2020 door gaat met haar missie ondernemend Nederland cyberweerbaar te maken. Het DTC wordt na 2020 een vast organisatieonderdeel van het Ministerie van Economische Zaken en Klimaat. Hiervoor is structureel budget beschikbaar. Daarnaast wordt momenteel voortvarend gewerkt door het Ministerie van EZK en JenV aan het laten voldoen van het DTC aan de wettelijke voorwaarden waardoor het DTC aangewezen kan worden als OKTT.

Ook het komende jaar zal Defensie de ingeslagen weg blijven volgen. Er worden meer mensen aangenomen en er wordt meer hard- en software aangeschaft om ook in het digitale domein antwoord te kunnen blijven geven op de dreigingen.

Zoals eerder gemeld is het streven om de actualisatie van het Nationaal Crisisplan Digitaal ter hand te nemen voor het einde van 2020.[3] Hierin kunnen de meest recente inzichten worden verwerkt, zoals bijvoorbeeld de lessen uit de evaluatie over de Citrix-problematiek van januari jl.

2. Bijdragen aan internationale vrede en veiligheid

Terugblik	- MBZ heeft tijdens de Algemene Vergadering van de VN in september 2019 samenwerking met Australië en de Verenigde Staten het Joint Statement on Advancing Responsible Behaviour in Cyberspace gepresenteerd. Deze verklaring is door 26 andere landen ondertekend. - Nederland zet zich in internationaal verband in voor versterking van coördinatie op het gebied van politieke attributie van cyberaanvallen. Een voorbeeld hiervan is de attributie van de cyberaanvallen op Georgië op 28 oktober 2019 aan de Russische militaire inlichtingendienst GROE. - De inlichtingen- en veiligheidsdiensten, BZ en de NCTV dragen actief bij aan een effectief attributiebeleid. - Als onderdeel van de EU cyberdiplomacy toolbox is mede op Nederlands initiatief in mei 2019 een EU-cybersanctieregime ingesteld, waarmee het mogelijk wordt om tegoeden te bevriezen en inreisverboden op te leggen. - In de Kamerbrief 'Internationale rechtsorde in het digitale domein' (medio 2019) zijn de internationaalrechtelijke regels (inclusief mensenrechten) die gelden in het digitale domein uiteengezet door het kabinet. - Medio 2019 zijn er consultaties met een groot aantal staten over de toepassing

[2] Kamerstukken II, 2019/20, 30 821, nr. 102.
[3] Kamerstukken II, 2019/20, 26643, nr. 685

	van het internationaal recht in het digitale domein georganiseerd. - Nederland heeft de GCSC ondersteund. De GCSC heeft in november 2019 het rapport 'Promoting stability in cyberspace to build peace and prosperity' gepubliceerd. - Het GFCE heeft eind 2019 een eigen juridische identiteit in de vorm van een stichting gekregen. Hiermee heeft het GFCE een brede internationale basis gekregen met publieke en private deelnemers, waardoor het GFCE meer toekomstbestendig is geworden. - Het cyberdiplomatennetwerk is verder versterkt. Daardoor wordt Nederland in staat gesteld cyber sneller en steviger bilateraal en multilateraal op de internationale agenda te positioneren binnen het diplomatieke domein. - Nederland heeft in maart een MoU getekend over de inzet van RRTs bij cyberincidenten en wederzijdse bijstand op het gebied van cyberbeveiliging binnen PESCO.
Vooruitblik	- Nederland zet in op de versterking van het diplomatiek responskader. Mede in navolging van de motie Verhoeven/Koopmans[4] zet Nederland zich in internationaal verband in voor versterking van coördinatie op het gebied van politieke attributie van cyberaanvallen. - Nederland blijft zich inzetten voor draagvlak voor een open, vrij en veilig internet, waar het bestaande internationaal recht van toepassing is en nageleefd wordt in bilateraal en multilateraal verband. Om dit te versterken zal Nederland de relatie met de 'swing states' intensiveren. - Defensie volgt internationale, conceptuele en juridische ontwikkelingen op de voet om van andere landen te leren, kaders op- of bij te stellen en mogelijk nieuwe inzetmogelijkheden vorm te geven, bijvoorbeeld voor de inzet van de RRTs. - Nederland blijft zich in het kader van het EU cybersanctieregime ook komend jaar inzetten om tegoeden te bevriezen en reisverboden op te leggen aan personen en entiteiten die zich schuldig maken aan ondermijnende cyberactiviteiten.

Uit het CSBN 2020 blijkt dat (voorbereiding van) sabotage en spionage door statelijke actoren een groot risico blijft voor de nationale veiligheid, en dat de digitale ruimte potentieel een terrein is voor conflicten tussen staten. Het kabinet blijft daarom investeren in internationale vrede en veiligheid in het digitale domein. Hierbij is het belangrijk om het diplomatiek responskader te versterken en het draagvlak voor een open, vrij en veilig internet te verbreden.

Nederland bevordert de internationale rechtsorde in het digitale domein en draagt bij aan het mitigeren van cyberdreigingen afkomstig van criminele en statelijke actoren. Het afgelopen jaar is op diverse vlakken geïnvesteerd in versterking van het diplomatiek responskader. De minister van Buitenlandse Zaken heeft tijdens de Algemene Vergadering van de VN in september 2019 een *Joint Statement on Advancing Responsible Behaviour in Cyberspace* in samenwerking met Australië en de Verenigde Staten gepresenteerd. Deze verklaring is vervolgens door 26 andere landen ondertekend. Hiermee heeft Nederland een leidende rol gespeeld bij het versterken van een internationaal normatief kader van regulering van cyberoperaties tussen staten. Om de internationale samenwerking ook in Europees verband verder te structuren, is op Nederlands initiatief een EU-cyberdiplomatie toolbox tot stand gekomen. Hiermee kunnen verschillende instrumenten van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid worden aangewend om degenen die ondermijnende cyberactiviteiten ontplooien ter verantwoording te roepen. Als onderdeel daarvan is mede op Nederlands initiatief in mei 2019 een EU-cybersanctieregime ingesteld waarmee het mogelijk wordt om tegoeden te bevriezen en inreisverboden op te leggen.[5]

[4] Kamerstukken II 2018/19, 33694 nr. 56

[5] Kamerstukken II 2018/19, 33694 nr. 47

Mede in navolging op de motie Verhoeven/Koopmans[6] zet Nederland zich in internationaal verband in voor versterking van coördinatie op het gebied van politieke attributie van cyberaanvallen. Een actueel voorbeeld hiervan is de attributie op 20 februari jl. door Nederland en gelijkgezinde landen van de cyberaanvallen op Georgië van 28 oktober 2019 aan de Russische militaire inlichtingendienst GROE.

Naast diplomatieke respons, is ook geïnvesteerd in verbreding van het draagvlak voor een open, vrij en veilig internet. In het kader van onderhandelingen in twee VN-fora heeft Nederland medio 2019 consultaties met een groot aantal staten over de toepassing van het internationaal recht in het digitale domein georganiseerd. Tevens zijn in de Kamerbrief internationale rechtsorde in het digitale domein medio 2019 de internationaalrechtelijke regels (inclusief mensenrechten) die gelden in het digitale domein uiteengezet.[7] Nederland draagt hiermee bij aan het vergroten van het interstatelijke draagvlak voor het open, vrije en veilige internet. Nederland acht betrokkenheid vanuit het bedrijfsleven, kennisinstellingen, de technische gemeenschap en maatschappelijk middenveld hierin van groot belang. Complementair aan de bestaande interstatelijke processen heeft NL daarom onder meer de Global Commission on the Stability of Cyberspace (GCSC) ondersteund. De GCSC heeft in november 2019 het rapport 'Promoting stability in cyberspace to build peace and prosperity' gepubliceerd. Daarnaast zet Nederland in op capaciteitsopbouw om het internationale draagvlak voor een open, vrij en veilig internet, waar het bestaande internationaal recht wordt gerespecteerd en geïmplementeerd, te verbreden. Middels het in 2015 door Nederland gelanceerde Global Forum on Cyber Expertise (GFCE) zijn strategische capaciteitsopbouw activiteiten ontplooid. Toepassing van internationaal recht op het digitale domein is een van de thema's waar het GFCE zich op richt. Aan de hand van de Tallinn Manual 2.05 worden wereldwijde capaciteitsopbouwprojecten uitgevoerd. Het GFCE heeft eind 2019 een eigen juridische identiteit in de vorm van een stichting gekregen. Hiermee heeft het GFCE een brede internationale basis gekregen met publieke en private deelnemers waardoor het GFCE meer toekomstbestendig is geworden en de internationale positie verder kan worden verbreed.

Zowel voor het verbreden van het draagvlak voor een open, vrij en veilig internet als voor versterking van diplomatieke respons op ongewenste statelijke cyberoperaties, is de inzet van het netwerk van Nederlandse diplomatieke vertegenwoordigingen van groot belang. Dit netwerk is op het terrein van cyberexpertise versterkt.

Vooruitblik
De komende periode wordt het diplomatiek responskader verder versterkt. Zo wordt het in EU-verband overeengekomen cybersanctieregime, als onderdeel van de brede geïntegreerde diplomatieke inspanning van de EU ter bevordering van internationale veiligheid en stabiliteit in cyberspace, zo spoedig mogelijk operationeel gemaakt. Mede in navolging op de motie Verhoeven/Koopmans[8] zet Nederland zich in internationaal verband in voor versterking van coördinatie op het gebied van politieke attributie van cyberaanvallen. Het kabinet wil vaker daders van cyberaanvallen publiekelijk aanspreken op hun gedrag. Dit vereist eerst technische attributie en vervolgens politieke en eventueel juridische attributie. Het vaststellen van wie de actor achter een cyberoperatie is, is daarvoor een onmisbare en complexe schakel die intensief onderzoek vergt. Een actief politiek attributiebeleid draagt bij aan het afschrikkend vermogen en het minder aantrekkelijk maken van Nederland als doelwit voor cyberaanvallen. Het publiekelijk attribueren van een actor is daarmee een van de diplomatieke middelen die Nederland tot zijn beschikking heeft.

Ook zal worden doorgegaan met het verbreden van het draagvlak voor een open, vrij en veilig internet, waar het bestaande internationaal recht van toepassing is en nageleefd wordt. NL blijft

[6] Kamerstukken II 2019/20, 33694 nr. 56
[7] Kamerstukken II 2019/20, 33694, nr. 47
[8] Kamerstukken II 2019/20, 33694, nr. 56

hierin een voortrekkersrol vervullen middels haar rol in de *UN Group of Governmental Experts* en de *UN Open Ended Working Group*, alsook via het door Nederland gelanceerde Global Forum on Cyber Expertise en het wereldwijde netwerk van Nederlandse 'cyberdiplomaten'.

3. Digitaal veilige hard- en software

Terugblik	- Het afgelopen jaar zijn in het kader van de Roadmap Digitaal Veilige Hard- en Software verdere stappen gezet in het verhogen van het niveau van cybersecurity van ICT-producten en diensten en het IoT waaronder: o In 2019 heeft de Europese Commissie impactstudies uitgevoerd naar het stellen van Europese wettelijke minimumeisen voor de cybersecurity van IoT-apparaten via de Radio Equipment Directive. o Ten aanzien van cybersecurity certificering is in 2019 de CSA van kracht geworden. o Het ministerie van EZK is november 2019 gestart met een campagne over het beveiligen van slimme apparaten door het doen van (onder andere) software updates. o In februari 2020 is een eerste versie opgeleverd van een handleiding ICO voor digitale producten en diensten. - Het NCSC heeft in 2019 een nieuwe versie van technische richtlijnen uitgebracht voor het zo veilig mogelijk configureren van het TLS. Dit protocol wordt gebruikt in allerlei communicatie toepassingen en is één van de fundamenten onder het internet.
Vooruitblik	- In het kader van de Roadmap Digitaal Veilige Hard- en Software: o Het risicomodel en de kwaliteitsregeling voor leveranciers van cybersecuritydiensten wordt medio 2020 opgeleverd. In de tweede helft van 2020 vinden pilots plaats en worden gewenste verbeteringen doorgevoerd. Begin 2021 vindt definitieve vaststelling en publicatie plaats. o In het kader van de Radio Equipment Directive zal de Europese Commissie in 2020 overgaan tot het formuleren van de noodzakelijke gedelegeerde handelingen. De Nederlandse inzet is dat de eisen eind dit jaar van kracht worden zodat op termijn voor alle met internet verbonden apparaten minimale digitale veiligheidseisen gelden. - De implementatie van CSA loopt en wordt de tweede helft van 2021 voltooid. - De ontwikkeling van Europese certificeringschema's is gestart voor onder andere clouddiensten. Nederland draagt via het publiek-private Partnering Trust bij aan de ontwikkeling van dit schema. - In de eerste helft van 2020 gaat BZK door middel van pilots ervaring opdoen met de wizard ICO, die als doel heeft dat aanbieders van hard- en software voldoen aan de inkoopeisen van de overheid.

Het digitaal veilig maken en houden van hard- en software is een van de belangrijke manieren om onze digitale weerbaarheid te vergroten. Niet voor niets worden onveilige producten en diensten in het CSBN 2020 de achilleshiel van de digitale veiligheid genoemd. Onveilige producten en diensten werken voor aanvallers drempelverlagend, omdat deze het makkelijker maken succesvolle aanvallen uit te voeren. Daarom is het de ambitie van dit kabinet om voorop te lopen in het bevorderen van digitaal veilige hard- en software. Belangrijke leidraad daarbij is de Roadmap Digitaal Veilige Hard- en Software (DVHS) die wordt uitgevoerd onder coördinatie van het Ministerie van Economische Zaken en Klimaat.

Het afgelopen jaar zijn in het kader van de Roadmap Digitaal Veilige Hard- en Software verdere stappen gezet in het verhogen van het niveau van cybersecurity van ICT-producten en diensten en het Internet of Things (IoT). In 2019 heeft de Europese Commissie impactstudies uitgevoerd naar het stellen van Europese wettelijke minimumeisen voor de cybersecurity van IoT-apparaten via de Radio Equipment Directive.

Ten aanzien van cybersecurity certificering is vorig jaar de Europese Cyber Security Act (CSA)[9] van kracht geworden. Deze verordening creëert een Europees raamwerk voor de certificering van ICT-producten, -diensten en –processen. Het creëert ook de plicht voor ieder lidstaat om een Nationale Cybersecurity Certificeringsautoriteit (NCCA) aan te wijzen. Hiervoor is nationale implementatiewetgeving nodig. Voor Nederland zal deze volgend jaar in werking treden. De Europese werkgroepen om te komen tot certificeringschema's zijn hun werk reeds gestart.

Aangezien bedrijven en organisaties primair voor hun eigen veiligheid en continuïteit verantwoordelijk zijn, is het van belang dat zij toegang hebben tot betrouwbare en kwalitatief goede private cybersecuritydienstverlening. Daarom heb ik samen met de staatssecretaris van Economische Zaken en Klimaat een subsidie aan het Centrum voor Criminaliteitspreventie en Veiligheid verstrekt om te komen tot een risicomodel, een kwaliteitsregeling en een certificeringsschema voor leveranciers van cybersecuritydiensten. Hiermee wordt een basisniveau van betrouwbaarheid en kwaliteit van cybersecuritydienstverleners bevorderd. Naar verwachting zullen het risicomodel en de kwaliteitsregeling medio dit jaar opgeleverd worden. In de tweede helft van 2020 vinden pilots plaats en worden de gewenste verbeteringen doorgevoerd. Begin 2021 vindt definitieve vaststelling en publicatie plaats.

De overheid kan met haar inkoopbeleid de vraag naar digitaal veilige ICT-producten en diensten stimuleren. In de eerste plaats omdat zij zelf veilig moet zijn. Maar ook kan zij als belangrijke afnemer van ICT-diensten bredere impact creëren. Door cybersecuritycriteria op te nemen in het inkoopbeleid moeten leveranciers van de overheid voldoen aan deze eisen. Hierdoor ontstaat een prikkel voor aanbieders om digitaal veilige producten en diensten op de markt te brengen. De overheid wil op deze wijze nadrukkelijk het goede voorbeeld geven. In februari 2020 is een eerste versie opgeleverd van een handleiding en een wizard Inkoopeisen Cybersecurity Overheid (ICO). Met de wizard is het mogelijk om eisenpakketten te selecteren die passen bij specifiek in te kopen producten-diensten.

Vooruitblik
In 2020 worden de aanvullende thema's voor de Inkoopeisen Cybersecurity Overheid (ICO) uitgewerkt van de wizard. Ook zijn dan de eisen voor standaardpakketten toegevoegd aan de wizard. Ook het toevoegen van eisen die gesteld kunnen worden bij de aanschaf van IoT-apparaten staat voor 2020 op de planning. Vanwege Europese ontwikkelingen op het terrein van IoT-apparaten zal de uitwerking van die betreffende eisen een langere doorlooptijd krijgen. Verder zal veel aandacht worden besteed aan het bevorderen van het gebruik van de wizard in inkoop en aanbestedingstrajecten, breed in de overheid. Onderdeel hiervan is ook het op gebruiksvriendelijk wijze aanbieden van de wizard via het internet.

In het kader van de Radio Equipment Directive zal de Europese Commissie naar verwachting dit jaar overgaan tot het formuleren van de noodzakelijke gedelegeerde handelingen. De Nederlandse inzet is dat de eisen eind dit jaar van kracht worden zodat op termijn voor alle met internet verbonden apparaten minimale digitale veiligheidseisen gelden. De ontwikkeling van Europese certificeringschema's onder de CSA is gestart voor onder andere clouddiensten. Nederland draagt via het publiek-private Partnering Trust bij aan de ontwikkeling van dit schema. Over de voortgang van alle maatregelen in de Roadmap Digitaal Veilige Hard- en Software zal uw Kamer in het najaar worden geïnformeerd door de staatsecretaris van EZK.

4. Beschikken over weerbare digitale processen en robuuste infrastructuur

[9] Kamerstukken II, 2018-2019 26643 nr. 618

Terugblik	- Het kabinet heeft de beleidsreactie op het WRR-rapport over digitale ontwrichting aan de Kamer aangeboden in maart 2020. - Het COT heeft een evaluatie over de aanpak van de Citrix-problematiek in januari jl. opgeleverd. - De consultatie van het concept-Bbni met daarin een verdere uitwerking van de zorgplicht uit de Wbni is afgerond. - IenW heeft de processen 'vervoer van personen en goederen over (hoofd)spoorweginfrastructuur' en 'vervoer over (hoofd)wegennet' (zie Kamerbrief TK 30821, nr. 108) als vitaal aangewezen. Daarnaast zijn organisaties in de chemische sector aangemerkt als vitaal. - Een verkenning door BZK van gebruik van vulnerabilityscanning binnen de rijksoverheid heeft geresulteerd in het voornemen om, in samenwerking met de Technische Universiteit Delft en NCSC een Rijksbreed kader voor vulnerability scanning te ontwikkelen. Dit moet leiden tot een meer gestandaardiseerde wijze van scanning, monitoring, kennisuitwisseling en aanpak van kwetsbaarheden. - Het NCSC is in pilotvorm gestart met het delen van informatie met toezichthouders in het geval van high/high-beveiligingsadviezen. Het NCSC heeft in dat kader onder andere toezichthouders op de hoogte gebracht van de kwetsbaarheid in Citrix ADC en Citrix Gateway. - Nederland draagt actief bij aan de verhoging van samenwerking op het gebied van digitale weerbaarheid binnen de EU via de Cooperation Group. Hierbinnen is Nederland co-voorzitter van verschillende werkgroepen, waaronder op het gebied van 5G en toezicht op digitale dienstverleners. - Onder Nederlands co-voorzitterschap heeft de Cooperation Group een Europese risico-analyse voor 5G en toolbox met mitigerende maatregelen opgeleverd. - De NVS is gepubliceerd, met daarin een versterkte aanpak voor beschermen van vitale infrastructuur. - De overheidsbrede cyberoefening: 'Wat zou jij doen?' specifiek gericht op overheden is georganiseerd door BZK in oktober 2019. - In februari 2020 is de geüpdate versie van de BIO gepubliceerd in het Staatscourant. - Met subsidie van BZK zijn drie gemeentelijke cyberoefeningen gefinancierd in februari 2020. Daarnaast zijn twee redteaming-oefeningen bij provincies en waterschappen gesubsidieerd.
Vooruitblik	- VWS voert een herbeoordeling uit om te bezien of bepaalde organisaties binnen de zorgsector als vitale aanbieders zouden moeten worden aangewezen. - IenW stelt sectorbeelden op om de cyberweerbaarheidsmaatregelen in kaart te brengen. In juni 2020 is de Tweede Kamer geïnformeerd over het eerste sectorbeeld over de voortgang van cybersecurity bij de sector water. - Het ontwerp van bovengenoemde wijziging van het Bbni wordt verder in procedure gebracht, en zal zo snel als mogelijk in werking treden. - Er worden verkenningen uitgevoerd naar o.a. de wettelijke taken en bevoegdheden bij incidenten met een digitale component. Op basis hiervan nodig gebleken wijzigingen van wetgeving worden in voorbereiding genomen. Daarnaast wordt een wijziging van de Wbni voorbereid die ertoe strekt ten aanzien van alle vitale aanbieders de in die wet geregelde plichten van toepassing te laten zijn.[10] - Binnen de EU wordt het komende jaar gewerkt aan een evaluatie van de NIB-richtlijn. - Nederland draagt in EU-verband bij aan de oprichting van het CyCLONe en de oefening Blue OLEx - De mogelijkheden om actuele dreigingsinformatie uit te wisselen tussen

[10] De reeds uitgezonderde sectoren blijven daarvan uitgezonderd.

	toezichthouders en het NCSC worden verder uitgewerkt. - Het coronavirus heeft gevolgen voor de voorbereiding en invulling van ISIDOOR 2020 en andere oefeningen. De cross-sectorale cyberoefening ISIDOOR zou dit jaar voor de derde keer worden gehouden, op 23, 24 en 25 juni. Vanwege de impact van dit virus wordt het uitgesteld naar een nader te bepalen datum in 2021. - Nederland neemt deel aan de Europese cyberoefening Cyber Europe in 2021 - In oktober 2020 vindt de tweede overheidsbrede cyberoefening plaats: "Wat heb jij gedaan?" specifiek gericht op overheden en georganiseerd door BZK. Dit jaar geheel virtueel vanwege de coronacrisis. - In 2020 zorgt BZK voor een hogere implementatiegraad van de BIO bij meer overheden. Naar aanleiding van de coronacrisis worden de activiteiten van het ondersteuningsprogramma versneld omgebouwd naar virtuele activiteiten in de vorm van onlinecursussen en Webinars. De bijbehorende producten worden zoveel als mogelijk digitaal beschikbaar gesteld. - In 2020 wordt de Kamer geïnformeerd over de uitkomsten van het onderzoek naar het altijd versleutelen van privacygevoelige gegevens in verhouding tot de BRP. - BZK onderzoekt op welke wijze informatieveiligheid in een volgende tranche van de Wet Digitale Overheid kan worden geborgd. - BZK verkent de wijze waarop de medeoverheden zijn toegerust op digitale ontwrichting en welke kaders en bevoegdheden nog nodig zijn.

Afgelopen jaar heeft het kabinet naast de reeds lopende trajecten uit de NCSA binnen ambitie vier, ook verschillende nieuwe maatregelen aangekondigd die bijdrage aan het realiseren van deze ambitie. Directe aanleiding van deze nieuwe maatregelen was het beeld van snel ontwikkelende dreiging en achterblijvende weerbaarheid dat geschetst werd in o.a. het CSBN2019[11] en het WRR-rapport: voorbereiden op digitale ontwrichting[12]. Alle maatregelen binnen deze ambitie dragen bij aan een verhoging van: (i) inzicht in de digitale weerbaarheid, (ii) de daadwerkelijke digitale weerbaarheid en (iii) het vermogen om snel in te kunnen grijpen bij digitale incidenten en de continuïteit van de dienstverlening te herstellen. Binnen deze ambitie moet daarnaast sprake zijn van een voortdurend proces van bijstellen van de weerbaarheid in het licht van de dreiging. Afgelopen jaar zijn in dit kader meerdere dingen gerealiseerd, maar er moeten ook nog flinke stappen gezet worden.

Zo wordt hard gewerkt aan de uitwerking van het oefenprogramma. Oefenen is namelijk één van de elementen die van belang is voor digitaal weerbare organisaties. Het kabinet zet in de uitwerking van het oefenprogramma in op drie sporen. Het eerste spoor bestaat uit het door dit kabinet organiseren van grootschalige oefeningen in het kader van het Nationaal Crisisplan Digitaal. Een voorbeeld hiervan is de cross-sectorale oefening ISIDOOR die gepland staat voor 2021. Een ander voorbeeld is 'De Overheidsbrede Cyberoefening' die door mijn collega van het ministerie van BZK wordt georganiseerd. Zoals reeds vermeld heeft COVID-19 impact op de planning en uitwerking van verschillende van deze initiatieven. Met subsidie van BZK zijn bovendien drie gemeentelijke cyberoefeningen gefinancierd in februari 2020. Het zijn een drietal oefeningen die alle gemeenten kunnen afnemen bij de VNG. Deze oefeningen zijn ontwikkeld door de VNG, op verzoek van BZK, in samenwerking met het COT Instituut voor Veiligheids- en crisismanagement. Het is een volledig cyberoefenpakket die toepasbaar is voor alle gemeenten in Nederland en gericht op het strategisch crisismanagement van de gemeente. Daarnaast zijn door BZK twee redteaming-oefeningen bij provincies en waterschappen gesubsidieerd. Het tweede spoor is de deelname van de overheid aan bestaande cyberoefeningen in verschillende sectoren. Zodoende kan gezamenlijk gewerkt worden aan de digitale weerbaarheid van organisaties. Het

[11] Kamerstukken II 2018/19, 26643, nr. 625

[12] Kamerstukken II, 2019/20, 26643, nr. 673

NCSC neemt bijvoorbeeld samen met partners zowel deel aan internationale oefeningen (zoals Cyberstorm en Cyber Europe) als aan nationale oefeningen (zoals ISIDOOR). Ook wordt regelmatig met samenwerkingspartners onderling geoefend. Het derde spoor is het ontwikkelen van initiatieven op oefeningen in publiek privaat verband om oefeningen in verschillende sectoren verder te stimuleren. Er wordt daarbij ook gekeken naar bestaande goede voorbeelden. De publiek private Cybersecurity Alliantie, waaraan ook vitale aanbieders deelnemen, speelt hierin een belangrijke rol. In dit kader zijn de eerste gesprekken gestart om deze initiatieven te ontwikkelen en verder te brengen. Daarnaast wordt ook gebruik gemaakt van het momentum rondom ISIDOOR om in gesprek te gaan met deelnemende vitale aanbieders over hoe we cyberoefeningen op basis van scenario's die aansluiten op het huidige dreigingsbeeld, zoals bijvoorbeeld geschetst in het CSBN, verder kunnen stimuleren. Met de verschillende partners worden de drie sporen verder uitgewerkt.

Een andere belangrijke stap is de doorontwikkeling van het wettelijk kader voor de beveiliging van onze netwerk en informatiesystemen. De consultatie van het Besluit netwerk en informatiesystemen (Bbni) is afgerond en het besluit gaat binnenkort de laatste fase van besluitvorming in. Hiermee wordt verder invulling gegeven aan de beveiligingsnormen voor Aanbieders van Essentiele Diensten (AEDs). Ook is er een wijziging van de Wet beveiliging netwerk- en informatiesystemen (Wbni) aangekondigd,[13] met als doel om alle vitale aanbieders onder het volledige regime van de Wbni te brengen.[14] Komend halfjaar zullen verschillende verkenningen afgerond worden die mogelijk verdere aanleiding geven tot wijziging van betrokken wetgeving, waaronder de Wbni. Met de voorbereidingen hiertoe is reeds gestart.

Naast het vergroten van de weerbaarheid van vitale processen is ook gewerkt aan het verbeteren van de weerbaarheid van de overheid zelf. De overheid heeft een bijzondere verantwoordelijkheid ten aanzien van de bescherming van persoonsgegevens en de te treffen beveiligingsmaatregelen. Voor deze bescherming is het van belang dat overheden permanent zorgdragen voor de integriteit van hun systemen en processen. Middels de Baseline Informatiebeveiliging Overheid (BIO) geven overheden (Rijk, provincies, gemeenten en waterschappen) daar uitwerking aan sinds 2019 (vaststelling BIO). In februari 2020 is de geüpdatete versie van de BIO gepubliceerd in het Staatscourant. Het tweejarig ondersteuningsprogramma BIO, om eraan bij te dragen dat alle overheden de BIO ook implementeren, vindt naast 2019 ook plaats in 2020 (het laatste ondersteuningsjaar).

Ten slotte zijn er belangrijke stappen gezet in het toezicht op en inzicht in onze digitale weerbaarheid. De afgelopen maanden is het NCSC in pilotvorm gestart met het delen van informatie met toezichthouders in het geval van high/high-beveiligingsadviezen. Het NCSC heeft in dat kader onder andere toezichthouders op de hoogte gebracht van de kwetsbaarheid in Citrix ADC en Citrix Gateway. De mogelijkheden om actuele dreigingsinformatie uit te wisselen tussen toezichthouders en het NCSC worden de komende periode verder uitgewerkt. Daarnaast hebben de toezichthouders gezamenlijk een eerste vertrouwelijk inspectiebeeld cybersecurity opgeleverd dat komend jaar verder wordt ontwikkeld met als doel meer zicht te krijgen op de staat van de digitale weerbaarheid voor wat betreft vitale aanbieders.

Ook in internationaal verband zet Nederland zich in voor samenwerking op het gebied van digitale weerbaarheid. Nederland is een actieve deelnemer binnen de Cooperation Group, waar lidstaten afspraken maken over de verdere uitwerking van de Netwerk- en Informatiebeveiligings (NIB)-richtlijn. Zo heeft Nederland een actieve rol in de werkgroepen over toezicht op digitale dienstverleners en over crisispreparatie. Binnen de werkgroep over de veiligheid van 5G-netwerken zijn onder Nederlands co-voorzitterschap een gemeenschappelijk risicobeeld en een toolbox met mitigerende maatregelen opgeleverd. Daarnaast zijn het NCSC en het CSIRT DSP

[13] Kamerstukken II, 2019/20, 26643, nr. 673

[14] De reeds uitgezonderde sectoren blijven daarvan uitgezonderd.

actief deelnemer aan het CSIRT Network, waar operationele informatie wordt uitgewisseld tussen CSIRTs. Nederland is dit jaar ook toegetreden tot de Executive Board van ENISA.

Vooruitblik
Bij het verschijnen van de kabinetsreactie op het WRR-rapport 'Voorbereiden op digitale ontwrichting' zijn er meerdere maatregelen aangekondigd die vallen binnen ambitie 4 van de NCSA. Voor het complete overzicht van deze maatregelen verwijs ik u graag naar de bijlage van de kabinetsreactie.[15]

De NCTV heeft stappen gezet in de ontwikkeling van de versterkte aanpak vitale infrastructuur waarover uw Kamer in de tweede helft van 2020 wordt geïnformeerd. VWS werkt aan een risico gestuurde aanpak om in kaart te brengen welke zorginstellingen het meeste cyberrisico lopen. Dit helpt om de Nederlandse zorgsector weerbaarder te maken. VWS voert daarnaast een herbeoordeling uit om te bezien of bepaalde organisaties binnen de zorgsector als vitale aanbieders zouden moeten worden aangewezen. Om bepaalde instellingen in de medische sector in Nederland die tijdens de COVID-19-crisis een belangrijke rol spelen zo weerbaar mogelijk te maken tegen digitale dreigingen, heb ik een spoedwetsvoorstel ingediend om het NCSC tijdelijk bijstand te kunnen laten verlenen aan deze instellingen.

In Europees verband is recent begonnen met de evaluatie van de Netwerk- en informatiebeveiligingsrichtlijn. De voorbereidingen voor het bepalen van een standpunt over deze evaluatie worden momenteel gestart.

Het ministerie van Infrastructuur en Waterstaat (IenW) laat sectorbeelden opstellen via een vertrouwelijk onderzoek naar cyberweerbaarheidsmaatregelen bij de sectoren waarvoor IenW (systeem)verantwoordelijkheid draagt. Deze beelden van de vitale sectoren waarvoor IenW uitvoeringsverantwoordelijkheid draagt zijn inmiddels opgeleverd. Het gaat hierbij bijvoorbeeld om keren en beheren (waterkwantiteit) en hoofdwegen. IenW informeert conform toezegging[16] de Kamer over de voortgang van cybersecurity bij sectoren waarvoor IenW (systeem)verantwoordelijkheid draagt. Dit zal via de geijkte kanalen gebeuren. Zo is de Tweede Kamer in het kader van het Algemeen Overleg Water van 22 juni 2020 per brief geïnformeerd over het eerste sectorbeeld, over de voortgang van cybersecurity in de watersector.

BZK onderzoekt in het kader van de BIO op welke wijze informatieveiligheid in een volgende tranche van de Wet Digitale Overheid kan worden geborgd (in ieder geval de BIO verplichten en toezicht voor vitale BZK-voorzieningen organiseren). Daarnaast worden in 2020 aanvullende thema's van het ICO uitgewerkt en wordt ingezet op het bevorderen van het breed gebruik van de cybersecurity eisen bij inkoop- en aanbestedingstrajecten in alle overheidslagen.

5. Succesvolle barrières opwerpen tegen cybercrime

[15] Kamerstukken II, 2019/20, 26643, nr. 673

[16] Handelingen II 2019/20 35300 XII; 35300 J, nr. 83

Terugblik	- Afgelopen jaar is opnieuw ingezet op preventie door een campagne tegen phishing en een campagne om daderschap onder de jeugd tegen te gaan. - In 2019 is door BZK interbestuurlijk verkend of het gebruik van één uniforme domeinnaamextensie bij de overheid (.overheid.nl) zou kunnen bijdragen aan de bestrijding van (spear)phishing en spoofing. - De consultatie van het conceptbesluit 'Besluit beveiligde verbinding met overheidswebsites en –webapplicaties' is afgerond. Het doel van dit voorgenomen besluit van BZK is om de toepassing van de informatieveiligheidsstandaarden HTTPS en HSTS verplicht te stellen voor publiek toegankelijke websites en webapplicaties van bestuursorganen.
Vooruitblik	- De Kamer wordt gelijktijdig met verschijning van het CSBN 2020 geïnformeerd over de voortgang van de integrale aanpak cybercrime - Om de adoptie van informatieveiligheidsstandaarden te vergroten, wordt, aanvullend aan de reguliere monitoring door het Forum Standaardisatie van BZK, in 2020 extra ingezet op voorlichting aan zogenaamde achterblijvers. Dit zal onder andere gebeuren via kanalen van BZK en het Forum Standaardisatie. - De open informatieveiligheidsstandaard HTTPS wordt verplicht om de beveiliging van overheidswebsites verder te bevorderen.

Het opwerpen van barrières tegen cybercrime blijft onverminderd belangrijk. Ambities zoals het meer digitaal vaardig maken van burgers en bedrijven (ambitie 6) en veilige hard- en software (ambitie 3) zorgen ervoor dat criminelen minder kans hebben. Daarnaast is reeds op 1 maart 2019 de wet Computercriminaliteit III in werking getreden. De Inspectie Justitie en Veiligheid is op dit moment bezig met het opstellen van haar verslag van haar toezicht en zal ingaan op de toepassing van de binnendringbevoegdheid in automatische werken door de politie. Het verslag zal ik deze zomer samen met mijn beleidsreactie naar de Kamer versturen. Eerder verwees ik al naar de sterke verwevenheid van cybersecurity en cybercrime op het terrein van preventie.[17] In het afgelopen jaar is opnieuw ingezet op preventie door onder meer een campagne tegen phishing en een campagne om daderschap onder de jeugd tegen te gaan. De activiteiten worden verder toegelicht in de brief integrale aanpak cybercrime. Deze brief gaat in op de verdere ontwikkeling van de integrale aanpak en wordt tegelijk met deze voorgangsbrief aan de Kamer gestuurd.

6. Toonaangevend op gebied cybersecurity kennisontwikkeling

Terugblik	- Als gevolg van de samenwerking in de NWA is er in december een call geopend van circa € 8 miljoen over cybersecurity-, governance- en cryptologievraagstukken. - NWO heeft eind 2019 ruim € 4 miljoen gehonoreerd aan 10 onderzoeksprojecten die binnen de call cybersecurity- digitale veiligheid & privacy zijn ingediend. - In juni 2019 is er vanuit de NWA € 8 miljoen gehonoreerd aan het onderzoeksproject INTERSECT. - Ten aanzien van het missiegedreven topsectoren- en innovatiebeleid is het afgelopen jaar zowel de KIA Veiligheid met de missie Cyberveiligheid, als de KIA Sleuteltechnologieën met een meerjarenprogramma cybersecurity ontwikkeld. - Samenwerking tussen overheden, bedrijven en kennisinstellingen is versterkt, via het missiegedreven topsectoren beleid, de nationale wetenschapsagenda, de uitgezette verkenningen en het Dutch Cybersecurity Platform for Higher Education and Research (Dcypher). - Er is een kwartiermaker aangesteld en gestart om de plannen voor een Cyber Innovation Hub nader vorm te geven. Dit volgt op de eerder uitgevoerde studie

[17] Kamerstukken II 2018/19, 26643, nr. 614

	hiernaar.
Vooruitblik	- Digitale geletterdheid wordt betrokken bij curriculumherziening voor het onderwijs onder de naam curriculum.nu. - Er komt een nieuw samenwerkingsplatform met een vervolgaanpak voor het versterken van cybersecurity kennisontwikkeling en innovatie, dat voortbouwt op Dcypher

Voor een digitaal veilige maatschappij is onze maatschappij afhankelijk van het ontwikkelen en toepassen van kennis. Dit is hard nodig om maatregelen te kunnen treffen tegen bestaande en nieuwe digitale dreigingen.[18] Bovendien voorkomt een hoogwaardige, autonome kennispositie een te grote afhankelijkheid van cybersecurity-expertise en cybersecurity-oplossingen uit andere landen.

Het kabinet heeft het afgelopen jaar via diverse impulsen cybersecurity kennisontwikkeling in Nederland versterkt. Zo is er in het afgelopen jaar in samenwerking tussen diverse departementen in het kader van de Nationale Wetenschapsagenda (NWA) meer dan € 20 miljoen euro beschikbaar gekomen dat geïnvesteerd is en wordt in cybersecurity kennisontwikkeling. Via het missiegedreven topsectoren- en innovatiebeleid is stevig ingezet op cybersecurity kennis- en innovatieontwikkeling. Zo wordt binnen de Kennis en Innovatieagenda Veiligheid[19] – onderdeel van het missiegedreven topsectoren en innovatiebeleid – specifiek de missie cyberveiligheid uitgevoerd. Via deze instrumenten investeert dit kabinet stevig op dit thema.

Verkenningen cybersecurity kennisontwikkeling en innovatie
Tegelijkertijd zijn in 2018 en 2019 door de betrokken departementen verkenningen uitgevoerd hoe de aanpak en samenwerking in Nederland verder versterkt kan worden. De staatssecretaris van EZK heeft uw Kamer hierover per brief geïnformeerd.[20] De essentie die uit al deze onderzoeken wordt gehaald, is de noodzaak om samenwerking over de hele keten heen te stimuleren door onder andere vraag en aanbod van kennis beter aan elkaar te verbinden en beter te coördineren.

Vooruitblik

Vervolgaanpak versterken cybersecurity kennisontwikkeling en innovatie
De aanpak ten aanzien van het versterken van het ecosysteem waar de staatssecretaris van EZK uw Kamer over heeft geïnformeerd, moet voorzien in een bredere, ketengeoriënteerde aanpak waarin bedrijven, kennisinstellingen en de overheid gezamenlijk inzetten op cybersecurityonderwijs, onderzoek en innovatie. De kern van deze nieuwe aanpak is dat het kabinet de ambities uit de verschillende beleidskaders, de Nederlandse Cybersecurity Agenda, de Defensie Cyber Strategie en de Nederlandse Digitaliseringsstrategie, voor cybersecurity wil realiseren door verschillende instrumenten, waaronder de Nationale Wetenschapsagenda en het missiegedreven topsectoren- en innovatiebeleid, in te zetten.

De basis voor de gezamenlijke vervolgaanpak zal bestaan uit een nieuw samenwerkingsplatform dat de krachten op het terrein van cybersecurityonderzoek, innovatie en onderwijs verder moet bundelen. Binnen dit samenwerkingsplatform komen alle relevante partijen, expertise, instrumenten en middelen uit het cybersecuritydomein bij elkaar. Deze aanpak bouwt voort op de ervaringen met en activiteiten van het Dutch Cybersecurity Platform for Higher Education and Research (Dcypher).

[18] Kamerstukken II 2018/19, 26643, nr. 614

[19] https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/KIA%20Veiligheid%20-%2020191016%20definitief.pdf

[20] Kamerstukken II 2019/20, 26643, nr. 674

Het samenwerkingsplatform zal door het ministerie van EZK verder uitgewerkt worden in samenwerking met de relevante departementen, kennisinstellingen en het bedrijfsleven.

Awareness cybersecurity
Ook dit jaar is door het ministerie van JenV in samenwerking met het ministerie van EZK ingezet op het creëren van meer bewustwording over veilig digitaal gedrag bij een breed publiek, bijvoorbeeld middels de campagnes 'Eerst checken dan klikken' en 'Doe je updates'. Ook het sinds 2012 bestaande initiatief 'Alert Online' zal dit jaar wederom doorgaan, met de piekperiode in de Cybersecurity Maand oktober. De website www.veiliginternetten.nl vormt de landingspagina voor de verschillende initiatieven die zo veel mogelijk in samenhang tot stand komen.

In het kader van de Roadmap Digitaal Veilige Hard- en Software is in november vorig jaar het kabinet begonnen met een campagne over de noodzaak van het regelmatig updaten van slimme apparaten. Verreweg de meeste slimme apparaten zijn te beveiligen met het doen van updates. Consumenten zijn hiervan maar beperkt op de hoogte. Mede daarom vormt het overbrengen van deze kennis een belangrijk onderdeel van de campagne en is van belang voor de digitale weerbaarheid van Nederland.

Digitale vaardigheden- cybersecurity en mediawijsheid
Met curriculum.nu wordt voor de eerste keer het gehele curriculum van primair en voortgezet onderwijs integraal en in samenhang tegen het licht gehouden. Opgenomen is het leergebied Digitale geletterdheid. Op dit moment vindt de concrete uitwerking plaats. In deze plannen is in ieder geval aandacht voor de opvolging van het advies van de Coördinatiegroep om digitale geletterdheid een integraal onderdeel van het curriculum voor het funderend onderwijs te maken en de lerarenopleidingen hier nauw in te betrekken. Het streven is om in samenwerking met lerarenopleidingen voorbeeldmaterialen en scholingsaanbod voor leraren te laten ontwikkelen.

7. Beschikken over een integrale, publiek-private aanpak van cybersecurity

Terugblik	- De Cyber Security Alliantie heeft diverse projecten afgerond of voortgezet: het opstellen van een roadmap t.b.v. de cyber weerbaarheid van ICS/SCADA-systemen, cybersecuritywoordenboek, veilige e-mailstandaarden en vulnerability management, TIBER-NL en Connect2Trust - NCSC heeft de handreiking 'Haal meer uit je ISAC' ontwikkeld. Op basis van de ervaringen van andere ISAC's heeft TNO in opdracht van het NCSC een ISAC-ontwikkelmodel opgesteld. Aan de hand van een checklist kan een ISAC een beeld krijgen van het huidige niveau en bepalen welke ambitie men nastreeft. - Het NCSC heeft samen met partnerorganisaties in Denemarken en de Verenigde Staten het initiatief genomen om met diverse andere landen een internationale coalitie te starten ter bevordering van de digitale weerbaarheid van de maritieme sector, waarin zowel publieke als private partijen betrokken zijn.
Vooruitblik	- De Cybersecurity Alliantie identificeert samen met haar deelnemers prioritaire thema's. Deze worden middels bundeling van de krachten verder ontwikkeld en leiden tot concrete output per thema in de komende periode. - In 2020 wordt door BZK een start gemaakt met een verkenning naar noodzakelijke kaders en afspraken in het kader van lokale ontwrichting door digitale incidenten. Dit wordt gedaan met gemeenten, provincies en waterschappen.

Om de doelstellingen van de NSCA te bereiken wordt op verschillende manieren samengewerkt. Deze samenwerking wordt vormgegeven door de publiek-private Cybersecurity Alliantie. De Cybersecurity Alliantie identificeert samen met haar deelnemers prioritaire thema's. Deze worden middels bundeling van de krachten verder ontwikkeld en leiden tot concrete output per thema in de komende periode. Afgelopen jaar heeft de Cyber Security Alliantie diverse projecten afgerond of voortgezet waaronder; het opstellen van een roadmap t.b.v. de cyber weerbaarheid van

ICS/SCADA-systemen, cybersecurity woordenboek, veilige e-mailstandaarden en vulnerability management, TIBER-NL en Connect2Trust.

Het NCSC heeft samen met partnerorganisaties in Denemarken en de Verenigde Staten het initiatief genomen om met diverse andere landen een internationale coalitie te starten ter bevordering van de digitale weerbaarheid van de maritieme sector. Vanwege de interconnectiviteit van het internationale maritieme transportsysteem is internationale samenwerking is cruciaal. Vanuit Nederland hebben veel verschillende publieke en private organisaties bijgedragen (Min IenW, RWS, Kustwacht, Defensie, NCTV, Havenbedrijf Rotterdam & Amsterdam).

Afgelopen jaar heeft het NCSC de handreiking 'Haal meer uit je ISAC' ontwikkeld, in zowel een Nederlandse als Engelse variant. Op basis van de ervaringen van andere ISACs heeft TNO in opdracht van het NCSC een ISAC-ontwikkelmodel opgesteld. Dit model vertaalt theorie naar de praktijk. Aan de hand van een checklist kan een ISAC een beeld krijgen van het huidige niveau en bepalen welke ambitie men nastreeft. Deze handreiking biedt tevens verschillende handvatten en hulpmiddelen die kunnen helpen bij de ontwikkeling van de ISAC. Ook is het NCSC als expert betrokken bij het vormgegeven van een EU ISAC model o.l.v. de Europese Commissie.

Vooruitblik
De Cybersecurity Alliantie identificeert de komende tijd samen met haar deelnemers prioritaire thema's voor concrete samenwerking. Deze worden middels bundeling van de krachten verder ontwikkeld en leiden tot concrete output per thema in de komende periode. Daarnaast wordt in 2020 door BZK een start gemaakt met een verkenning naar noodzakelijke kaders en afspraken in het kader van lokale ontwrichting door digitale incidenten. Dit wordt gedaan met gemeenten, provincies en waterschappen.

Afkortingen

AEDs	Aanbieders van Essentiele Diensten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
Bbni	Besluit beveiliging netwerk- en informatiesystemen
BIO	Baseline Informatiebeveiliging Overheid
BRP	Basisregistratie Personen
BZ	Ministerie van Buitenlandse Zaken
BZK	Ministerie van Binnenlandse Zaken en Koninkrijkrelaties
CERT	Computer Emergency Response Team
CERT- WM	Computer Emergency Response Team Water Management
COT	Instituut voor Veiligheids- en Crisismanagement
CSA	Cyber Security Act
CSBN	Cybersecurity Beeld Nederland
CSIRT	Computer Security Incident Response Team
CSIRT DSP	Computer Security Incident Response Team voor digitale dienstverleners
CSR	Cyber Security Raad
CyCLONe	Cyber Crisis Liaison Officers Network
DCC	Defensie Cyber Commando
DCSC	Defensie Cyber Security Centrum
DTC	Digital Trust Center
DVHS	Roadmap Digitaal Veilige Hard- en Software
ENISA	Europees Agentschap voor netwerk- en informatiebeveiliging
EU	Europese Unie
EZK	Ministerie van Economische Zaken en Klimaat
GCSC	Global Commission on the Stability of Cyberspace
GFCE	Global Forum on Cyber Expertise
GROE	Glavnoje Razvedyvatelnoje Oepravlenije
HTTPS	HyperText Transfer Protocol Secure

HSTS	HTTP Strict Transport Security
ICO	Inkoopeisen Cybersecurity Overheid
ICS/SCADA	Supervisory Control And Data Acquisition
ICT	Informatie en Communicatietechnologie
IenW	Ministerie van Infrastructuur en Waterstaat
IoT	Internet of Things
ISAC	Information Sharing Analysis Center
JenV	Ministerie van Justitie en Veiligheid
KIA Veiligheid	Kennis en Innovatieagenda Veiligheid
LDS	Landelijke Dekkend Stelsel
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MoU	Memorandum van overeenstemming
NBIP	Nationale Beheersorganisatie Internet Providers
NCCA	Nationale Cybersecurity Certificeringsautoriteit
NCSA	Nederlandse Cybersecurity Agenda
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NDN	Nationaal Detectie Netwerk
NIB-richtlijn	Netwerk- en informatiebeveiligingsrichtlijn
NVS	Nationale Veiligheidsstrategie
NWA	Nationale Wetenschapsagenda
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek
OKTT	objectief kenbaar tot taak
OM	Openbaar Ministerie
PESCO	Permanent Structured Cooperation
RRTs	Rapid Response Teams
RWS	Rijkswaterstaat
SURFcert	Computer Emergency Response Team voor bij SURF aangesloten instellingen
TLS	Transport Layer Security-protocol
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek
VN	Verenigde Naties
VNG	Vereniging van Nederlandse Gemeenten
VWS	Ministerie van Volksgezondheid, Welzijn en Sport
WRR	Wetenschappelijke Raad voor het Regeringsbeleid
Wbni	Wet beveiliging netwerk- en informatiesystemen
Z-CERT	Zorg- Computer Emergency Response Team