Bijlage: Voortgangsrapportage NCSA 2021

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	- Instellen van de Cyber Info/Intel Cel, waarbinnen AIVD, MIVD, NCSC, OM en politie dreigingsinformatie bijeenbrengen, medewerkers van deze organisaties die informatie gezamenlijk beoordelen, en van waaruit informatie aan belanghebbende organisaties kan worden verstrekt. - Een Nationale Cryptostrategie is opgesteld, waarmee de ontwikkeling van gerubriceerde beveiligingsproducten voor de Rijksoverheid een belangrijke impuls krijgt. - Het Nationale Detectie Netwerk (NDN) is verder doorontwikkeld en het aantal deelnemers aan het NDN is verder uitgebreid. Vanuit de NCTV, NCSC, MIVD en AIVD zijn ten behoeve van de verdere uitwerking van een toekomstbestendig NDN twee werkgroepen (voor de korte en lange termijn) ingericht. - AIVD en MIVD zijn gestart met de ontwikkeling van een gezamenlijk dataplatform ter ondersteuning van inlichtingenonderzoek. - Inmiddels zijn er 36 samenwerkingsverbanden bij het Digital Trust Center (DTC) aangesloten. Website, sociale media en een digitaal platform van het DTC zijn verder doorontwikkeld. Het DTC heeft in 2020 diverse interactieve tools ontwikkeld zoals het Risicoklassemodel (in samenwerking met het Centrum voor Criminaliteitspreventie en veiligheid) en een wegwijzer voor cybersecurityinitiatieven (in samenwerking met het CIO Platform). Een basisscan veilig ondernemen is doorontwikkeld om te komen tot meer gebruikersgemak. Ter vergroting van het bereik en effect van het DTC is een strategisch communicatieplan opgesteld. - Defensie heeft haar Cyber Threat Intelligence-capaciteit vergroot door aan te sluiten op het Threat Intelligence Platform van het NCSC. Mede hierdoor is Defensie tijdig in staat te reageren op nieuwe dreigingen en kwetsbaarheden. Dit jaar zal het TIP verder worden geïntegreerd binnen het DCSC. - Abuse Information Exchange, NBIP, Cyberweerbaarheidscentrum Brainport, Cyberveilig Nederland, Connect2Trust en FERM zijn krachtens de Wbni aangewezen als OKTT, waardoor zij van het NCSC specifieke informatie kunnen ontvangen. - Het NCSC is in gesprek met de Veiligheidsregio's (onder coördinatie van het IFV) en provincies (samen met BZK) om ten behoeve van die partijen schakelorganisaties aan te sluiten op het landelijk dekkend stelsel (LDS). - Het NCSC faciliteerde de Information Sharing and Analysis Centres (ISACs) en nam als partij ook deel aan deze platformen voor informatie- en expertisedeling van de verschillende sectoren. Om te bevorderen dat er meer cross sectoraal wordt samengewerkt en uitgewisseld vindt inmiddels twee keer per jaar een collectieve bijeenkomst plaats van alle ISAC-vertegenwoordigers. De ISACs zijn gewaardeerde platformen van de sectoren en het NCSC zet ook in 2021 in op versterking van de werking van de ISACs en de rol van het NCSC daarin. - Ten aanzien van de energiesector faciliteert het NCSC een afzonderlijk digitaal platform voor het zo veel als mogelijk delen van cyberdreigingsinformatie onder netbeheerders. Dit platform heeft als doel om op een snelle en effectieve wijze IOC's (indicators of compromise) te delen en verrijken. Met het platform kan informatie over sectorspecifieke dreigingen gerichter worden gedeeld en verrijkt. Uitkomsten kunnen daarnaast door het NCSC worden benut voor andere sectoren. Het digitale platform is als afzonderlijk onderdeel gepositioneerd binnen het Nationaal Detectie Netwerk en is in samenwerking tussen het NCSC en de brancheorganisatie voor netbeheerders ontwikkeld. - AIVD en MIVD hebben meer personeel aangenomen en hebben daardoor meer capaciteit en middelen om onderzoek te doen, en om de resultaten van dit onderzoek met relevante partijen te delen. - Het Defensie Cyber Commando (DCC) gaat richting volledige personeelsvulling. Hierdoor kunnen operationele eenheden worden gereedgesteld ter afschrikking,

	voor missies en kunnen operationele cybercapaciteiten verder ontwikkeld worden. Hierbij wordt intensief samengewerkt met de inlichtingen- en veiligheidsdiensten. - De actualisering van het Nationaal Crisisplan Digitaal is ter hand genomen. - Het NCSC verleent dankzij de in de Tweede Verzamelspoedwet COVID-19 geregelde tijdelijke aanpassing van de Wbni bijstand aan onder meer instellingen waar intensive care wordt verleend, instellingen die onderzoek doen betreffende de diagnostiek van COVID-19 en fabrikanten van geneesmiddelen.

Het CSBN 2021 schetst dat de digitale dreiging zich blijft doorontwikkelen, met mogelijk grote economische en maatschappelijke gevolgen bij incidenten. Door het vergroten van de digitale slagkracht van Nederland verhoogt het kabinet de weerbaarheid tegen deze dreiging. In de afgelopen periode is de slagkracht versterkt door het verbeteren van de samenwerking tussen verschillende overheidspartijen en het verbeteren van de aansluiting op elkaars systemen. Zo is in 2020 officieel de Cyber Info/Intel Cel van start gegaan, waarbinnen AIVD, MIVD, NCSC, OM en politie dreigingsinformatie bijeenbrengen en medewerkers van die organisaties structureel op één fysieke locatie bij het NCSC die informatie gezamenlijk beoordelen, waardoor er sneller een beeld is van nieuwe dreigingen en belanghebbende organisaties meer en sneller van handelingsperspectief kunnen worden voorzien.

De AIVD en MIVD hebben hun capaciteit verder uitgebreid en hebben daardoor meer cyberonderzoek kunnen uitvoeren. Met cyberonderzoek wordt beoogd inlichtingenposities te realiseren ten aanzien van uitvoerders en opdrachtgevers van hoogwaardige digitale aanvallen die een bedreiging vormen voor de Nederlandse nationale veiligheid. Daarmee wordt zicht verkregen op huidige en toekomstige digitale aanvallen, op de oogmerken, doelwitten en de gebruikte modus operandi (digitale infrastructuur en uitvoering van de "kill-chain") bij die digitale aanvallen. Detectie van digitale aanvallen maakt Nederland veiliger, beschermt de democratische rechtsorde en stelt de nationale belangen veilig. Afgelopen periode is specifiek geïnvesteerd in detectie, monitoring en het verkrijgen van informatie via (commerciële) cyberbronnen.

Door de vergroting van de digitale slagkracht draagt Defensie bij aan een effectief en serieus afschrikkingsbeleid. Het kunnen uitvoeren van offensieve cyberoperaties hoort hier ook bij. Hiervoor ontwikkelt het DCC capaciteiten die binnen de juridisch-ethische kaders kunnen worden ingezet. De komende periode zal Defensie onderzoeken wat de mogelijkheden en beperkingen in het cyberdomein zijn en hoe Defensie de juridische mogelijkheden optimaal kan gebruiken bij gereedstelling en inzet.

Het DTC wordt steeds bekender als informatieknooppunt voor het niet-vitale bedrijfsleven (zie ook de Kamerbrief van 16 december 2020). Het aantal samenwerkingsverbanden groeit ook gestaag, met als gevolg een groter bereik in diverse regio's, sectoren en branches. Voor het delen van algemene informatie en advies zijn de website, sociale media en een digitaal platform verder doorontwikkeld en ingezet. Thema-specifieke mini-campagnes (op onderwerpen zoals thuiswerken en back-ups maken) dragen bij aan een groter bereik bij de DTC-doelgroep (niet-vitaal bedrijfsleven). Samen met onder meer het Centrum voor Criminaliteitspreventie en Veiligheid en het CIO platform zijn diverse praktische tools voor ondernemers ontwikkeld. Deze tools helpen ondernemers wegwijs in cybersecurityland én geven inzicht in de eigen cyberweerbaarheid en wat verder te doen staat. Door het ministerie van EZK wordt gewerkt aan het laten voldoen van het DTC aan de voorwaarden waardoor het DTC krachtens de Wbni als OKTT kan worden aangewezen. Om de juridische basis voor het verwerken van persoonsgegevens te versterken is ten behoeve daarvan gestart met het opstellen van een wetsvoorstel. Daarnaast is eind 2020 ook gestart met de inrichting van een informatiedienst voor het delen van concrete risico-informatie met individuele bedrijven. Voornemen is om in de zomer binnen de huidige (juridische) mogelijkheden met de informatiedienst te starten. Hierover bent u recent door het ministerie van EZK geïnformeerd[1].

Het kabinet heeft, conform eerdere toezeggingen aan uw Kamer[2], de actualisering van het Nationaal Crisisplan Digitaal ter hand genomen. Het plan zal nog dit jaar worden beoefend tijdens de nationale en cross-sectorale cyberoefening ISIDOOR 2021. Eventuele relevante bevindingen en

[1] Kamerstukken II 2020/2021, 26643, nr. 760

[2] Kamerstukken II 2020/2021, 26643, nr. 738.

lessen uit deze oefening worden meegenomen bij de actualisering. Ook dit plan wordt omgevormd naar een landelijk crisisplan en het streven is om dit na de zomer op te leveren.

Het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden blijft in ontwikkeling. In publicaties over het LDS worden zaken die verbetering behoeven en kansen benoemd in de verdere doorontwikkeling van het stelsel. Hierover heb ik u geïnformeerd in mijn beleidsreactie op het in opdracht van het WODC uitgevoerde onderzoek naar mogelijkheden voor de doorontwikkeling van het LDS[3]. Binnen het staande beleid wordt in interdepartementaal verband en met externe partijen verkend welke sectoren in onze samenleving niet goed zijn aangesloten en waar cybersecurity informatiedeling en het verhogen van de weerbaarheid van toegevoegde waarde is.

2. Bijdragen aan internationale vrede en veiligheid

Terugblik	- Defensie en BZ hebben ingezet op deelname aan verschillende Europese PESCO-initiatieven op het gebied van cybersecurity, zoals de PESCO Cyber Rapid Response Teams. - Defensie en BZ hebben een bijdrage geleverd aan beleidsvorming van de NAVO omtrent digitale inzet. - Eind 2020 is het Cyber Crises Liaison Organisation Network (CyCLONe) officieel opgericht tijdens de door Nederland georganiseerde cyberoefening Blue OLEx 2020. CyCLONe is een nieuw EU-cybercrisismanagementnetwerk dat tot doel heeft om op tactisch/strategisch niveau uitwisseling tussen lidstaten te stimuleren om het niveau van paraatheid te verhogen en een gezamenlijk situationeel beeld te ontwikkelen ten tijde van grootschalige ICT incidenten. CyCLONe complementeert de bestaande cybersecurity crisismanagement structuren op EU-niveau en vormt de verbindende schakel tussen het technische niveau (EU CSIRT Netwerk) en het politieke niveau (geïntegreerde regeling politieke crisisrespons [IPCR]). - BZ heeft de Nederlandse visie op internationaal recht in het digitale domein effectief ingebracht in multilateraal verband (o.a. VN en OVSE) t.b.v. draagvlak voor een normatief kader voor gedrag van (niet-)statelijke actoren in cyberspace. - BZ heeft de (inter)nationale coördinatie van politieke attributie van cyberaanvallen versterkt. Met politieke attributie wordt een aantal doelen gediend, waaronder: het benadrukken van het belang dat wij hechten aan het normatief kader voor cyber space, het verhogen van de prijs van onwenselijk gedrag in cyber en het verhogen het publieke bewustzijn over cyberdreigingen. - In relatie daarmee heeft BZ een leidende rol gespeeld bij het opzetten van het EU-cybersanctieregime in 2019 en de verlenging hiervan in 2021, om zo gezamenlijk de kosten van onwenselijk gedrag in cyberspace te verhogen. - De samenwerking tussen de EU en de NAVO op het gebied van cyber is versterkt rondom de thema's digitale weerbaarheidsverhoging en respons op kwaadaardige cyberoperaties. - BZ heeft bijgedragen aan versterking en verbreding van like-minded coalities naar like-minded en swing states coalities dankzij dialogen met belangrijke swing states. - Via partnerschappen en samenwerking met andere stakeholders, zoals het Global Forum on Cyber Expertise, heeft BZ de Nederlandse inzet op het thema gender en cyber verder uitgerold. - BZ heeft een leidende rol in de Freedom Online Coalition gespeeld door op nieuwe onderwerpen (AI en desinformatie) te werken aan gezamenlijke verklaringen met normatieve richtlijnen conform het mensenrechtenraamwerk. - BZ heeft bijgedragen aan de internationale kennisuitwisseling over cybersecurity (m.i.v. kritieke technologieën) en desinformatie. - Het cyberdiplomatennetwerk van BZ is verder versterkt. Daardoor wordt Nederland in staat gesteld effectiever internationaal overleg te voeren over cyber. - BZ heeft capaciteitsopbouwprogramma's op het gebied van normen en internationaal recht in het digitale domein en technische weerbaarheid versterkt,

[3] Kamerstukken II 2020/2021, 26643, nr. 722

	o.a. via het door Nederland opgerichte Global Forum on Cyber Expertise en de OVSE.

Het CSBN2021 geeft aan dat de toegenomen digitalisering en technologische mogelijkheden de digitale risico's vergroten. Doelwitten van statelijke en criminele actoren zijn vaak digitaal benaderbaar en het plegen van een cyberaanval is relatief laagdrempelig en goedkoop. Internationale samenwerking is een basisvoorwaarde om hier weerstand tegen te bieden en de integriteit van de digitale ruimte te bewaken.

Eind maart jl. heeft de Europese Raad conclusies aangenomen over de EU-strategie inzake cyber-beveiliging voor het digitale decennium. Hierin is de Nederlandse inzet meegenomen conform BNC fiche[4]. Om de ontwikkeling, uitvoering en monitoring van deze voorstellen te waarborgen is gevraagd aan de Commissie en de hoge vertegenwoordiger een gedetailleerd uitvoeringsplan op te stellen en zal Nederland binnen de Raad toezien op de uitvoering door middel van een actieplan.

Defensie en BZ zoeken in internationaal verband aansluiting bij lopende initiatieven zoals de PESCO Cyber Rapid Respons Teams en spreken in NAVO-verband over beleidsvorming omtrent digitale inzet en de rol van het bondgenootschap.

Op 22 oktober maakte de EU nieuwe sancties bekend onder het EU-cybersanctieregime. De sancties betroffen twee Russische personen en een Russische organisatie die betrokken waren bij cyberoperaties gericht tegen het Duitse parlement in 2015. Op 19 oktober maakte de VS aanklachten bekend tegen dezelfde actor. Deze aanklachten hadden betrekking op een groot aantal cyberaanvallen, onder meer op de Franse verkiezingen van 2017 en de Olympische Winterspelen van 2018. De minister van Buitenlandse Zaken reageerde op de EU-sancties en de aanklachten vanuit de VS en gaf hiermee een krachtig signaal af, waarin EU en trans-Atlantische gelijkgezindheid ten aanzien van dit soort cyberaanvallen werd benadrukt. BZ heeft een leidende rol gespeeld bij het opzetten van het EU-cybersanctieregime in 2019 en de verlenging hiervan in 2021, om zo gezamenlijk de kosten van onwenselijk gedrag in cyberspace te verhogen.

In maart 2021 werd consensus bereikt onder alle VN-lidstaten over verantwoordelijk statelijk gedrag in cyberspace. Met het consensusrapport van de Open Ended Working Group herbevestigen alle VN-lidstaten de centrale rol voor het internationaal recht en zijn Nederlandse prioriteiten omarmd. Alle VN-lidstaten kunnen nu worden gehouden aan deze maatstaf van verantwoord gedrag in cyberspace.

Verder heeft BZ bijgedragen aan versterking en verbreding van like minded coalities naar like minded en swing states coalities dankzij dialogen met belangrijke swing states. In 2020/2021 vonden de eerste regionale cyberdialogen plaats in onder meer de Indo-Pacific regio en Zuidelijk Afrika.

3. Digitaal veilige hard- en software

Terugblik	- Het raamwerk voor veilige softwareontwikkeling van de publiek-private *Secure Software Alliance* is het afgelopen jaar geïmplementeerd bij International Card Services (ICS) en de Universiteit Wageningen en onderdeel geworden van het curriculum bij NCOI en de Universiteit van Antwerpen. - Het wetsvoorstel richtlijnen verkoop goederen en levering digitale inhoud van het ministerie van EZK is dit jaar aangeboden aan de Kamer. Hierdoor hebben consumenten recht op (veiligheids-) updates zolang zij die redelijkerwijs mogen verwachten. - Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) heeft een cybersecurity risicomodel ontwikkeld in opdracht van de ministeries van EZK en JenV. Naast een objectief oordeel over het niveau van cyberrisico van een (mkb-)onderneming, biedt het instrument inzicht in de bijpassende beheersmaatregelen. - Daarnaast heeft het CCV een keurmerk gelanceerd voor pentesten. Aanbieders van pentest-diensten kunnen zich op basis daarvan laten certificeren, wat voor de afnemer duidelijkheid verschaft over de kwaliteit van de af te nemen dienst. - Er zijn cybersecurity inkoopeisen voor alle overheidsorganisaties ontwikkeld in opdracht van de ministeries van BZK en EZK Via het online-instrument

[4] Kamerstukken 2020/2021, 22112, nr. 3052

	Inkoopeisen Cybersecurity Overheid (ICO inkoopwizard) is dit nu gemakkelijk toegankelijk en snel te raadplegen. - Er zijn Europese raadsconclusies aangenomen in de Telecomraad in december 2020 die het belang van de cybersecurity van verbonden apparaten benadrukken

In het kader van de Roadmap Digitaal Veilige Hard- en Software (DVHS) is het afgelopen jaar met publiek en private partners in Nederland en de EU doorgebouwd aan het verhogen van het maatschappelijke niveau van digitale veiligheid van ICT-producten en diensten inclusief het *Internet of Things* (IoT). Over de voortgang van alle maatregelen bent u op 14 december 2020 geïnformeerd door de staatssecretaris van EZK[5]. Op 7 december 2020 heeft de Europese Telecomraad raadsconclusies aangenomen om de cybersecurity van verbonden apparaten te benadrukken. In de raadsconclusies is opgeroepen om aanvullend aan andere maatregelen horizontale wet- en regelgeving te ontwikkelen voor verbonden apparaten[6].

Het wetsvoorstel 'Richtlijn verkoop goederen en Richtlijn levering van digitale inhoud' van het ministerie van EZK implementeert twee Europese richtlijnen op het gebied van consumentenbescherming[7]. Het wetsvoorstel is eerder dit jaar aangeboden aan de Kamer. Dit wetsvoorstel expliciteert onder meer een verplicht updateregime voor digitale inhoud en tastbare goederen met een digitaal element. Consumenten hebben hiermee recht op (veiligheids-) updates zolang zij die redelijkerwijs mogen verwachten. De verkoper/handelaar zal afspraken moeten maken met een derde, zoals de fabrikant of een softwareleverancier, die de updates kunnen leveren. Uitzondering hierop is wanneer de handelaar bij de aankoop de consument er expliciet op wijst dat hij geen updates mag verwachten, en de consument hiermee instemt.

In opdracht van de ministeries van EZK en JenV heeft het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) in samenwerking met diverse private partijen de Risicoklasseindeling Digitale Veiligheid ontwikkeld, vindbaar op de website van het DTC. Hiermee kunnen ondernemers hun risicoprofiel met bijbehorende te nemen maatregelen bepalen. Daarnaast is het door het CCV ontwikkelde Certificatieschema Pentesten in april 2021 gepubliceerd[8]. Aanbieders van pentesten kunnen zich op basis hiervan laten certificeren. Dit verschaft duidelijkheid voor de afnemer over de kwaliteit van de dienst. Naar verwachting zal rond de zomer het eerste certificaat Pentesten worden uitgereikt.

Het raamwerk voor veilige softwareontwikkeling van de publiek-private *Secure Software Alliance* is het afgelopen jaar na succesvolle pilots in zijn geheel geïmplementeerd bij International Card Services (ICS) en de Universiteit Wageningen en onderdeel geworden van het curriculum bij NCOI en de Universiteit van Antwerpen. Onder andere Rabobank en KPN verkennen de implementatie van het raamwerk.

De verwachting is dat de Europese Commissie dit jaar de noodzakelijke gedelegeerde handelingen publiceert waarmee wettelijke digitale veiligheidseisen worden gesteld aan slimme apparaten onder de *Radio Equipment Directive* (RED). Daarna zal een overgangsperiode starten waarbinnen de Europese standaardisatieorganisaties de benodigde technische standaarden zullen uitwerken en fabrikanten zich kunnen voorbereiden. Nederland wil een leidende rol spelen in deze ontwikkelingen. Het ministerie van EZK ondersteunt met subsidie het Nederlandse normalisatie instituut NEN het Nederlandse voorzitterschap van een Europese CEN/CENELEC werkgroep voor IoT-veiligheid. Na de overgangsperiode van de cybersecurityeisen onder de RED kunnen producten die niet voldoen aan de cybersecurity eisen van de markt worden geweerd en gehaald door Agentschap Telecom.

De Europese Cybersecurity Act (Cyberbeveiligingsverordening, CSA) creëert een Europees stelsel van cybersecurity certificering voor ICT-producten, -diensten en -processen. De eerste Europese cybersecurity certificeringschema's zijn in ontwikkeling, waaronder voor clouddiensten. Nederland draagt met de Online Trust Coalitie vanuit publieke en private expertise bij aan de ontwikkeling

[5] Kamerstukken II 2020/2021, 26643, nr. 735

[6] Kamerstukken II 2020/2021, 2150133, nr. 838

[7] Kamerstukken II 2020/2021, nr. 35734

[8] Zie https://hetccv.nl/keurmerken/expert/keurmerk-pentesten

van het certificeringschema voor clouddiensten. Nederland implementeert de CSA via het wetsvoorstel Uitvoeringswet cyberbeveiligingsverordening voor het inrichten van het certificeringstelsel in Nederland en wijst Agentschap Telecom aan als de nationale autoriteit en toezichthouder. Het wetsvoorstel is aangeboden aan de Kamer[9].

Ten aanzien van cybersecurity inkoopeisen voor de overheid zijn dit jaar pilots bij verschillende overheidsorganisaties uitgevoerd, waaronder bij ICTU en Logius. De pilots hebben een positief beeld opgeleverd over de praktische uitwerking van de cybersecurity inkoopeisen en de inzet van het tool (ICO-wizard) in de praktijk. De definitieve versie van het tool is online beschikbaar[10]. De doelstelling blijft om deze cybersecurity inkoopeisen te gaan hanteren voor alle overheidslagen als een uitwerking van de Baseline Informatiebeveiliging Overheid (BIO). Ze vormen nadrukkelijk onderdeel van het BIO-versnellingsprogramma dat het ministerie van BZK in 2021 uitvoert. De ministeries van BZK en EZK hebben in samenwerking met de medeoverheden cybersecurity inkoopeisen ontwikkeld voor alle overheidsorganisaties.

4. Beschikken over weerbare digitale processen en robuuste infrastructuur

Terugblik	- Wijziging van Besluit beveiliging netwerk- en informatiesystemen is per 1 mei en 1 juni 2021 in werking getreden[11]. Hiermee worden nadere regels gesteld over de plicht voor AED's om passende en evenredige beveiligingsmaatregelen te nemen; voorts worden hiermee enkele nieuwe AED's (waarvoor naast de zorgplicht ook een meldplicht van ernstige incidenten bij de toezichthouder en het NCSC geldt) en andere vitale aanbieders (waarvoor een meldplicht bij het NCSC van ernstige incidenten met geldt) aangewezen. - Een verkenning is uitgevoerd naar de wettelijke taken en bevoegdheden van de rijksoverheid met betrekking tot informatiedeling en interventie bij digitale dreigingen of incidenten bij vitale aanbieders, niet-vitale organisaties en rijksoverheidsorganisaties. - Door het programma 'versterken weerbaarheid in de watersector' wordt de cyberweerbaarheid in deze sector verhoogd. Daarnaast is door IenW ook voor de andere sectoren waar zij systeemverantwoordelijk over is cyberbeelden opgesteld. Van elke sector is inzicht ontstaan met betrekking tot de cybersecurity en wat de verbeterpunten zijn. De cyberbeelden dienen als input voor het doorontwikkelen van de cyberstrategie van het ministerie van IenW. - De in 2019 vastgestelde Baseline Informatiebeveiliging Overheid (BIO) is verder onder de aandacht gebracht door het ministerie van BZK door middel van gerelateerde hulpmiddelen, webinars en handreikingen. - Verdere inzet op oefenen en testen is voortgezet via het oefen- en testprogramma, waar o.a. de nationale cyberoefening ISIDOOR 2021, georganiseerd door NCSC en NCTV, onderdeel van uitmaakt. - BZK heeft cyberoefenpakketten opgesteld voor gemeenten en provincies, waarmee cyberincidenten kunnen worden doorlopen. - De NCTV is gestart met het ontwikkelen van een versterkte aanpak voor de bescherming van de vitale infrastructuur. De versterkte aanpak zet in op het versterken van het huidige Rijksbrede programma 'weerbare vitale infrastructuur' door o.a. het huidige instrumentarium en de governancestructuren te actualiseren en toekomstbestendig te maken. - De NCTV heeft eind september 2020 de virtuele cybercrisisoefening Blue OLEx georganiseerd. Blue OLEx is een cybersecurityoefening op strategisch niveau voor de executives van CyCLONe (directeuren nationale cybersecurity autoriteiten). Blue OLEx heeft tot doel het vertrouwen te versterken tussen lidstaten, de Europese Commissie en ENISA voor versterkte samenwerking ten tijde van grootschalige ICT-incidenten, en de algemene paraatheid voor grootschalige ICT-incidenten te oefenen. - Eind december 2020 heeft de Europese Commissie een voorstel tot herziening van de Netwerk- en informatiebeveiligingsrichtlijn (NIB-richtlijn) gepubliceerd. De kabinetspositie voor de Nederlandse inzet voor de onderhandeling hierover is

[9] Kamerstukken II 2020/2021, nr. 35838

[10] Zie https://www.bio-overheid.nl/ico-wizard/

[11] Staatsblad (2021, 160)

	in februari 2021 naar de Tweede Kamer verzonden.[12] Interdepartementaal worden onder coördinatie van de NCTV voorbereidingen getroffen voor de verdere onderhandelingen en de latere implementatie in nationale wetgeving. - EZK en NCTV hebben in het kader van de NIB Samenwerkingsgroep afgelopen jaar verder gewerkt aan de implementatie van verschillende maatregelen uit de EU 5G security toolbox. Lidstaten kunnen de toolbox gebruiken als handvat om nationale maatregelen vorm te geven. In juni 2020 is een EU voortgangsrapportage verschenen over welke maatregelen uit de 5G toolbox lidstaten implementeren en de wijze waarop. Eind december is als onderdeel van het EU cybersecurity pakket een evaluatie van het EU 5G toolbox proces gepubliceerd inclusief aanbevelingen[13].

In het afgelopen jaar zijn verschillende stappen gezet om de weerbaarheid van de Nederlandse vitale infrastructuur te verhogen. Het CSBN2021 schetst dat de weerbaarheid in vitale processen in Nederland soms tekort schiet en dat het risico bestaat dat vitale processen, zoals de distributie van elektriciteit, ontoegankelijk worden als gevolg van (voorbereidingen voor) sabotage en de inzet van ransomware. Gezien deze dreiging zet het kabinet onder meer in op het (door)ontwikkelen van sectorspecifieke maatregelen, zodat per sector gekeken wordt op welke manier de weerbaarheid het meest effectief verhoogd kan worden.

Eveneens zet dit kabinet in op het oefen- en testprogramma. Oefenen is één van de elementen die van belang is voor digitaal weerbare organisaties. Het kabinet zet in de uitwerking van het oefenen daarbinnen 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. Op 1, 2, 3 en 10 juni heeft in dat kader de cross-sectorale oefening ISIDOOR plaatsgevonden waarin dit plan werd beoefend. Deze oefening is georganiseerd door het NCSC en de NCTV. Een ander voorbeeld is 'De Overheidsbrede Cyberoefening' die door mijn collega van het ministerie van BZK in oktober 2021 voor de derde keer wordt georganiseerd. 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 derde spoor is het ontwikkelen van initiatieven op oefeningen in publiek privaat verband om oefeningen in verschillende sectoren verder te stimuleren. De publiek private Cybersecurity Alliantie, waaraan ook vitale aanbieders deelnemen, speelt hierin een belangrijke rol. Zo is via de Alliantie samengewerkt aan een Oefentool om organisaties te helpen bij het organiseren van een cyberoefening. Deze oefentool is op korte termijn beschikbaar op de website van de alliantie. Daarnaast is ook in aanloop naar ISIDOOR, via o.a. masterclasses en scenariowerkgroepen, tussen deelnemende publieke en private partners informatie gedeeld over een goede voorbereiding op een digitale crisis.

In het kader van het oefen- en testprogramma wordt ook ingezet op testen. Het testen van een digitale infrastructuur en processen is belangrijk omdat daarmee inzicht ontstaat in de effectiviteit van genomen beveiligingsmaatregelen. Om organisaties te helpen heeft het NCSC een Whitepaper Security Testen gepubliceerd op haar website. Dit document biedt een handleiding voor organisaties voor het kiezen en opzetten van verschillende types security tests. Deze is openbaar beschikbaar. Ook op de website van het DTC is informatie voor niet-vitale organisaties te vinden over testen. Eisen t.a.v. testen zijn onderdeel van de Baseline Informatievoorziening Overheid (BIO), het basisnormenkader voor alle overheidsorganisaties. Een groot aantal informatiebeveiligings- hulpmiddelen en -producten zijn ontwikkeld, verzameld en ontsloten via het BIO-portaal www.bio-overheid.nl. Op dit portaal zijn bijv. webinars en handreikingen te vinden. Overheidsorganisaties worden hiermee praktisch geholpen en ook geïnspireerd op het gebied van informatieveiligheid.

Een andere belangrijke stap is de doorontwikkeling van het wettelijk kader voor de beveiliging van netwerk- en informatiesystemen. Per 1 mei en 1 juni jl. is een wijziging van het Bbni in werking getreden. Hiermee worden nadere regels gesteld met betrekking tot de plicht voor AED's om passende en evenredige beveiligingsmaatregelen te nemen. Daarnaast worden hiermee verschillende nieuwe AED's en andere vitale aanbieders (AVA's) aangewezen.

[12] Kamerstukken II 2020/2021, 22112, nr. 3053

[13] Kamerstukken II 2020/2021, 21501 33, nr. 823

Naar aanleiding van het WRR-rapport 'Voorbereiden op digitale ontwrichting' heeft het kabinet de wettelijke taken en bevoegdheden van de rijksoverheid in kaart gebracht met betrekking tot informatiedeling en interventie bij digitale dreigingen of incidenten bij vitale aanbieders, niet-vitale organisaties en rijksoverheidsorganisaties[14]. Ook is geïnventariseerd of en in welke zin aanvullingen hierop nodig zijn. Uit deze verkenning is gebleken dat er reeds diverse wettelijke taken en bevoegdheden zijn om vanuit de overheid informatie over digitale dreigingen en incidenten te kunnen delen met rijksoverheid, vitale en niet-vitale organisaties. Ten aanzien van interventiemogelijkheden is er op basis van de verkenning geen reden om te concluderen dat er in de Wbni dan wel in sectorale wetgeving ten aanzien van vitale aanbieders bevoegdheden ontbreken. Uit de verkenning is ook gebleken dat de overheid mogelijkheden heeft om in buitengewone omstandigheden in te grijpen bij aanbieders die niet als vitaal zijn aangemerkt. Met betrekking tot de bevoegdheden tot het delen van informatie is echter uit de verkenning gebleken dat er op dit moment in sommige gevallen nog geen een wettelijke grondslag voor het NCSC bestaat om dreigings- en incidentinformatie over netwerk- en informatiesystemen van andere aanbieders dan die in de doelgroep van Rijk en vitaal, die door het NCSC is verkregen in het kader van de primaire taakuitoefening, aan of ten behoeve van deze aanbieders te verstrekken. Zoals vermeld in mijn antwoorden op vragen van het lid Yesilgöz-Zegerius van 29 maart 2021 werk ik aan een wetsvoorstel tot wijziging van de Wbni, waardoor het NCSC de hiervoor bedoelde informatie bij die andere aanbieders terecht kan laten komen[15]. Dit voorstel houdt concreet in dat het NCSC ook aan OKTT's vertrouwelijke herleidbare informatie over aanbieders kan verstrekken, zodat deze schakelorganisaties de aanbieders in hun doelgroepen van relevante dreigings- en incidentinformatie kunnen voorzien. Daarnaast houdt het voorstel in dat het NCSC in bijzondere gevallen informatie kan verstrekken aan organisaties die geen deel uitmaken van de doelgroep van Rijk en vitaal. Ik streef ernaar om dit wetsvoorstel rond de zomer in consultatie te brengen.

5. Succesvolle barrières opwerpen tegen cybercrime

Terugblik	- Voor extern gerichte overheidswebsites wordt het gebruik van HTTPS verplicht. - Er zijn meerdere activiteiten ter voorkoming van slachtofferschap en daderschap van cybercrime ondernomen. - De evaluatie van de Wet Computercriminaliteit III is gestart. Deze wordt naar verwachting eind 2021 gepubliceerd. - Zie voor de voortgang van de integrale aanpak cybercrime de gelijknamige brief die gelijktijdig met deze voortgangsrapportage met uw Kamer is gedeeld.

Tussen het versterken van de cybersecurity en de aanpak van cybercrime bestaan raakvlakken. Het verhogen van de digitale vaardigheden van burgers en bedrijven is hierbij belangrijk. Om deze reden zijn ook afgelopen jaar meerdere activiteiten uitgevoerd gericht op het voorkomen van dader- en slachtofferschap van cybercrime. Zo is bijvoorbeeld opnieuw ingezet op het tegengaan van daderschap via een campagne waarbij ook scholen worden betrokken en is gestart met een pilot voor een 'cyberweerbericht' (zie onder ambitie 7).

De Wet Computercriminaliteit III is inmiddels twee jaar in werking. De bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk heeft geleid tot mooie successen. Zo is de bevoegdheid ingezet in de internationale politieoperatie LadyBird, waarbij de servers achter de schadelijke malware Emotet uit de lucht zijn gehaald. De wetsevaluatie van CCIII is gestart en wordt naar verwachting in het voorjaar 2022 afgerond. De integrale aanpak van cybercrime is breder en omvat tevens diverse activiteiten die geen directe relatie hebben met de nationale veiligheid. Het totale pakket aan maatregelen binnen de integrale aanpak van cybercrime wordt nader toegelicht in de Kamerbrief hierover. Deze wordt net zoals voorgaande jaren tegelijkertijd met deze voortgangsbrief aan de Kamer gestuurd

6. Toonaangevend op gebied cybersecurity kennisontwikkeling

Terugblik	- Een nieuw publiek-privaat samenwerkingsplatform is opgericht, DCypher, waarin de gehele cybersecurity kennis- en innovatieketen wordt samengebracht. Door op deze manier partijen, middelen, instrumenten en expertise te bundelen kan de impact van alle betrokken organisaties sterk worden vergroot.

[14] Kamerstukken 2020/2021, 26643, nr. 738

[15] Aanhangsel Handelingen 2020/2021, nr 2173

	- In 2020 heeft het ministerie van EZK de Nationale Wetenschapsagenda call 'Cybersecurity, governance- en cryptologievraagstukken' opgehoogd met €1,5 miljoen. Deze onderzoekscall van circa 9,5 miljoen wordt door zeven verschillende ministeries gefinancierd (waarvan 3 miljoen van OCW via NWO). - Digitale geletterdheid is meegenomen in de herziening van het curriculum van het basisonderwijs en voortgezet onderwijs, dat in de komende periode verder zal worden uitgewerkt. - Een pilot is gestart om te komen tot een 'cyberweerbericht', een nieuwsbericht over het actuele digitale dreigingsbeeld en bijpassende handelingsperspectieven voor burgers en bedrijven.

EZK heeft in samenwerking met andere departementen inmiddels via diverse impulsen kennisontwikkeling in Nederland versterkt. Eind 2019 en begin 2020 zijn door de betrokken departementen een aantal verkenningen uitgevoerd hoe de aanpak en samenwerking in Nederland verder versterkt kan worden. De uitkomsten van de analyses en de knelpunten die door de betrokkenen zijn aangedragen worden herkend. De essentie die uit al deze onderzoeken worden 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. Het kabinet heeft daarom voorgesteld om een nieuw publiek-privaat samenwerkingsplatform op te richten dat de maatschappelijke krachten op het terrein van onderzoek, innovatie en onderwijs moet bundelen. Het platform heet Dcypher en dient relevante partijen, expertise, instrumenten en middelen uit het cybersecurity domein bij elkaar te brengen in een thematische en ketengeoriënteerde aanpak. De doelstellingen van Dcypher zijn:

- Er zijn voldoende goed opgeleide cybersecurity mensen in Nederland;
- We genereren internationaal leidende expertise in cybersecurity in Nederland;
- Deze expertise leidt tot effectieve toepassing in Nederlandse producten en diensten.

Op basis van een adviesrapport, opgesteld door vijf kwartiermakers uit overheid, bedrijfsleven en wetenschap, is EZK in 2020 gestart met de oprichting van DCypher. Een platformmanager is aangenomen om sturing te geven aan de activiteiten van het samenwerkingsplatform. Het ondersteunend platformbureau is ondergebracht bij de Rijksdienst voor Ondernemend Nederland (RVO). Er is een bestuur samengesteld met vertegenwoordigers vanuit alle betrokken partijen. Samen met partners uit het veld is een inhoudelijke start gemaakt met twee thematische pilot roadmaps op de onderwerpen Automated Vulnerability Research en Cryptocommunicatie. De website Dcypher.nl is in het voorjaar live gegaan.

Begin 2021 is gestart met de inhoudelijke inventarisatie, met als doel de samenwerking te structureren via thematische communities en via routekaarten te komen tot concrete en gedragen programma's en projecten. Verwachting is dat in de loop van 2021 het aantal routekaarten zal groeien, samen met het aantal betrokken partners. Ten slotte wordt op termijn de aansluiting gezocht op Europese initiatieven en instrumenten via het 'national coordination centre'. Door dit centre aan te sluiten op het samenwerkingsplatform wordt een directe link gelegd met het Europese Cybersecurity Competence Centre (ECCC) en het bijbehorende netwerk. Het ECCC moet de beschikbare expertise op het gebied van cybersecurity onderzoek gaan bundelen en de Europese cybersecurity community bij elkaar gaan brengen. Ook zal het centrum verantwoordelijk zijn voor het verdelen van de middelen die vanuit Horizon Europe en Digital Europe beschikbaar worden gemaakt voor innovatie op het gebied van cybersecurity.

Digitale geletterdheid is nog geen onderdeel van het curriculum van het basis- en voortgezet onderwijs. De afgelopen jaren hebben leraren en schoolleiders, daarbij ondersteund door andere experts, in negen ontwikkelteams voorstellen opgeleverd voor de herziening van het curriculum in het basisonderwijs (po) en voor de onderbouw van het voortgezet onderwijs (vo). Voor de eerste keer wordt het gehele curriculum van primair en voortgezet onderwijs integraal en in samenhang tegen het licht gehouden. 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. Eerder heeft ook de Cyber Security Raad geadviseerd om, als onderdeel van een integrale aanpak cyberweerbaarheid, meer aandacht te geven aan digitale geletterdheid in het onderwijs[16]. Als eerste vervolgstap is een wetenschappelijke curriculumcommissie ingesteld die de

[16] Zie https://www.cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

minister gaat adviseren over de opgeleverde bouwstenen. Ook adviseert de commissie over de werkopdracht aan SLO. Beide adviezen volgen in januari 2021. Op basis daarvan gaan kerndoelenteams in één jaar tijd de bouwstenen voor po en onderbouw-vo ontwikkelen tot conceptkerndoelen. Vanaf 2021 gaat ook de herziening van de eindtermen van de bovenbouw van het vo van start.

In het AO cybersecurity van 9 december vorig jaar heeft het lid Van Dam (CDA) de suggestie gedaan om te komen tot 'cyberweerbericht': een periodiek nieuwsbericht over het actuele dreigingsbeeld en bijpassende handelingsperspectieven gericht op burgers, maar ook op bedrijven, zodat ze daarop alert kunnen zijn. Op dit moment loopt er een pilot van de Politie samen met de Fraudehelpdesk en veiliginternetten.nl waarbij een maandelijks (trend)bericht over actuele criminele werkwijzen wordt gepubliceerd. Deze pilot is in maart gestart en loopt tot en met mei. Deze pilot wordt geëvalueerd en op basis van de resultaten daarvan zal worden gekeken of het cyberweerbericht zal worden gecontinueerd en zo ja in welke vorm.

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

Terugblik	- Binnen de Cybersecurity Alliantie zijn verschillende thematische werkgroepen actief waarbij op uiteenlopende cybersecurity onderwerpen wordt samengewerkt, zoals op het gebied van ICS/SCADA-systemen. Voor het thema oefenen wordt bijvoorbeeld gewerkt aan een interactieve tool om het opzetten van cyberoefeningen te ondersteunen. - Het via de Cyber Security Alliantie en onder leiding van Cyberveilig Nederland opgestelde 'cybersecurity woordenboek' is verder doorontwikkeld en wordt onder de aandacht gebracht. In het woordenboek is een verklarende woordenlijst opgesteld met bijna 600 cybersecuritytermen om bijvoorbeeld rapporten, adviezen of offertes beter te begrijpen. - Het WODC heeft een brede evaluatie uitgevoerd van de NCSA, met als doel om te reflecteren op de achterliggende beleidstheorie en de mogelijkheden voor een effectevaluatie te onderzoeken. - Het NCSC participeert aan en faciliteert de Anti-DDos Coalitie, een samenwerkingsverband van publieke, private en wetenschappelijke partijen waarbinnen informatie en kennis over DDOS-aanvallen zo veel als mogelijk en op laagdrempelige wijze gedeeld wordt. - Het NCSC verdiept de samenwerking met een aantal Nederlandse multinationals in een samenwerkingsverband (zogenaamde Circle of Trust). Op deze manier versterkt het NCSC de eigen informatiepositie en worden deze organisaties (en hun ketens) zo veel als mogelijk geholpen beter weerbaar te worden. Het is momenteel in gesprek met hen over mogelijkheden om een schakelorganisatie op te richten die vervolgens krachtens de Wbni als OKTT aangewezen kan worden. - Het NCSC ondersteunt partijen momenteel bij het opzetten van een ISAC voor de semi-conductor industrie. - Met cybersecurityvendoren (via Cyberveilig Nederland) start NCSC een Proof of Concept om door middel van tooling het NCSC in het kader van zijn taakuitoefening geheel anoniem informatie te kunnen laten delen. Op deze manier wil het NCSC sneller zicht krijgen op relevante ontwikkelingen en dit zo veel als mogelijk en efficiënt delen met partijen. Als dit succesvol blijkt wil het NCSC deze tooling ook inzetten in de samenwerking met andere partijen.

De NCSA vormt een integrale aanpak, waarbij op veel verschillende onderwerpen tussen publieke en private partijen wordt samengewerkt. In de terugblik van de ambities zoals hierboven beschreven komt dit ook meermaals terug. In vrijwel alle ambities komen initiatieven langs waar de overheid in overleg met het bedrijfsleven of ander organisaties samenwerkt om de weerbaarheid tegen cyberdreigingen te verhogen. Dit geldt specifiek voor de Cybersecurity Alliantie, die tot doel heeft om in publiek-privaat verband te kijken naar mogelijkheden om de Nederlandse cybersecurity te verbeteren. Op verschillende thema's wordt in de Alliantie samengewerkt, bijvoorbeeld op het gebied van ICS/SCADA-systemen en het uitleggen van cyberterminologie.

Het NCSC is actief in de Anti-DDoS-Coalitie. Dit is een samenwerkingsverband van publieke, private en wetenschappelijke partijen waarbij informatie en kennis over DDoS aanvallen zo veel als mogelijk op laagdrempelige wijze gedeeld kan worden, waardoor de weerbaarheid tegen

aanvallen verhoogd wordt. Met name de intensiteit en complexiteit van de aanvallen c.q. aanvalsvectoren neemt toe. Daarom wordt in het kader van de Anti-DDoS-Coalitie steeds gewerkt aan nieuwe voorzieningen, zoals een uitwisselingsplatform om technische kenmerken van DDoS-aanvallen nog sneller te delen. Het NCSC is deelnemer aan de coalitie en aanjager hiervan. Daarnaast levert het NCSC aan de coalitie specialistische kennis en probeert het NCSC andere sectoren en organisaties te verbinden aan de coalitie. Ten slotte speelt het NCSC zijn internationale schakelrol bijvoorbeeld bij aanvallen.

Het in publiek-privaat verband samenwerken vormt onderdeel van de integrale aanpak zoals vastgelegd in de NCSA, dat het cybersecuritybeleid van het kabinet als geheel uiteenzet. Doordat ontwikkelingen in het cyberdomein zich snel opvolgen is het daarbij van belang om kritisch te blijven kijken naar de huidige aanpak. Het WODC is daarom gevraagd om een evaluatie uit te voeren van de NCSA. Het WODC concludeert dat de opzet van de NCSA in algemene zin logisch is, met een opbouw van doelstellingen, ambities en maatregelen, maar ook dat er verbetermogelijkheden zijn. Op het moment dat een volgend kabinet besluit over de opvolging van de NCSA is het onder meer van belang om aandacht te geven aan de meetbaarheid van de (verwachte) effecten van de strategie, zodat het effect van cybersecuritybeleid in een toekomstige evaluatie beter inzichtelijk wordt. Ook de overige aanbevelingen zullen in de gedachtevorming over de opvolging van de NCSA worden meegenomen. Het evaluatierapport van NCSA is op 11 juni met u gedeeld[17].

Afkortingen

AEDs	Aanbieders van essentiële diensten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
Bbni	Besluit beveiliging netwerk- en informatiesystemen
BIO	Baseline Informatiebeveiliging Overheid
BZ	Ministerie van Buitenlandse Zaken
BZK	Ministerie van Binnenlandse Zaken en Koninkrijkrelaties
CERT	Computer Emergency Response Team
CSA	Cybersecurity Act
CSBN	Cybersecurity Beeld Nederland
CSIRT	Computer Security Incident Response Team
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
GFCE	Global Forum on Cyber Expertise
HTTPS	HyperText Transfer Protocol Secure
ICO	Inkoopeisen Cybersecurity Overheid
ICT	Informatie en Communicatietechnologie
IenW	Ministerie van Infrastructuur en Waterstaat
IoT	Internet of Things
JenV	Ministerie van Justitie en Veiligheid
LDS	Landelijke Dekkend Stelsel
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NBIP	Nationale Beheersorganisatie Internet Providers
NCSA	Nederlandse Cybersecurity Agenda
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NDN	Nationaal Detectie Netwerk
NIB-richtlijn	Netwerk- en informatiebeveiligingsrichtlijn
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek
OKTT	Organisatie die objectief kenbaar tot taak heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere

[17] Kamerstukken II 2020/2021, nr. 10605

	netwerk- en informatiesystemen [dan die van vitale aanbieders en van andere aanbieders die onderdeel zijn van de rijksoverheid]
OM	Openbaar Ministerie
PESCO	Permanent Structured Cooperation
RRTs	Rapid Response Teams
SLO	Stichting Leerplanontwikkeling
VN	Verenigde Naties
VWS	Ministerie van Volksgezondheid, Welzijn en Sport
Wbni	Wet beveiliging netwerk- en informatiesystemen