Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

26 643 **Informatie- en communicatietechnologie (ICT)**

30 821 **Nationale Veiligheid**

Nr. 685

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 28 mei 2020

De vaste commissie voor Justitie en Veiligheid heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Justitie en Veiligheid over de brief van 23 januari 2020 inzake «Overzicht op hoofdlijnen Citrix-kwetsbaarheden» (Kamerstuk 26 643, nr. 660), over de brief van 11 februari 2020 inzake «Analyse van de gelopen risico's door de kwetsbaarheden in de virtual private network (VPN) software van het bedrijf Pulse Secure» (Kamerstuk 26 643, nr. 666), over de brief van 13 februari 2020 inzake «Verzoek aan de commissie over het aanhouden van een verslag van schriftelijk overleg over het overzicht op hoofdlijnen Citrix-kwetsbaarheden» (Kamerstuk 26 643, nr. 667) en over de brief van 20 maart 2020 inzake «Kabinetsreactie op het rapport «Voorbereiden op digitale ontwrichting» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en een overzicht van de geleerde lessen van de Citrix-problematiek» (Kamerstukken 26 643 en 30 821, nr. 673).

De vragen en opmerkingen zijn op 17 april 2020 aan de Minister van Justitie en Veiligheid voorgelegd. Bij brief van 25 mei 2020 zijn de vragen beantwoord.

De voorzitter van de commissie,
Van Meenen

Adjunct-griffier van de commissie,
Burger

kst-26643-685
ISSN 0921 - 7371
's-Gravenhage 2020

Inhoudsopgave

I. Vragen en opmerkingen vanuit de fracties

1. Inleiding

De leden van de VVD-fractie hebben kennisgenomen van de geagendeerde brieven voor het schriftelijk overleg Cybersecurity en hebben hier nog enkele vragen en opmerkingen over.

De leden van de PVV-fractie hebben kennisgenomen van de brieven die zijn geagendeerd voor het schriftelijk overleg Cybersecurity. Zij hebben nog vragen over de brief «kabinetsreactie op het rapport «Voorbereiden op digitale ontwrichting» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en een overzicht van de geleerde lessen van de Citrix-problematiek».

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van de agenda en stukken van het schriftelijk overleg cybersecurity. Zij hebben enkele vragen.

De leden van de GroenLinks-fractie hebben met interesse kennisgenomen van de verschillende brieven over cybersecurity, met name over de Citrix-kwetsbaarheid en over het rapport «Voorbereiden op digitale Ontwrichting» van de WRR. De huidige crisis rond de COVID-19 pandemie laat eens te meer het belang zien van een zo goed mogelijke voorbereiding op crisissituaties. Voornoemde leden hebben nog enkele vragen bij de verschillende brieven.

2. Overzicht op hoofdlijnen Citrix-kwetsbaarheden

De leden van de VVD-fractie brengen in herinnering dat een lek in de software van het Amerikaanse bedrijf Citrix eerder dit jaar grote gevolgen heeft gehad voor thuiswerkers, zorginstellingen, gemeenten, universiteiten en talloze andere bedrijven en organisaties. Vanwege zwakke plekken in de beveiliging konden hackers in minder dan een minuut tijd toegang krijgen tot het interne netwerk. Ook ministeries werden hiermee geconfronteerd. U beschrijft dat het Nationaal Cyber Security Centrum (NCSC) op 17 december 2019 op de hoogte werd gebracht van de kwetsbaarheid van het Citrix-systeem. Citrix maakte op dat moment publiekelijk bekend dat sprake was van een kwetsbaarheid. De tijdlijn daarna roept bij de aan het woord zijnde leden enkele vragen op. Zo heeft het NCSC pas vanaf 9 januari 2020 vitale gebruikers van Citrix actief publiekelijk geïnformeerd over de kwetsbaarheden. Kunt u aangeven waarom hier drie weken tussen zat? Hoe beoordeelt u het feit dat de vitale gebruikers niet meteen zijn geïnformeerd door het NCSC over de kwetsbaarheden? Kunt u aangeven welk protocol gevolgd dient te worden

in geval van een lek in het Citrix-systeem? Is dit protocol correct opgevolgd?
Constaterende dat het lek in Citrix vanaf 17 december 2019 bekend was bij het NCSC en dat het NCSC op 17 januari 2020 het advies aan vitale aanbieders en de rijksoverheid had uitgegeven om het Citrix-systeem uit te schakelen, vragen voornoemde leden in hoeverre de rijksoverheid en vitale aanbieders die gebruik maken van het Citrix-systeem risico hebben gelopen. Kunt u hier een onderbouwde risicoanalyse van geven?
De leden van de VVD-fractie vragen ook welke concrete maatregelen naast het informeren van vitale aanbieders door het NCSC zijn genomen tussen het publiekelijk informeren over de kwetsbaarheden op 9 januari 2020 en het advies met betrekking tot het afsluiten van het Citrix systeem uitgeven op 17 januari 2020.
Voornoemde leden lezen dat u tevens schrijft dat sectorale toezichthouders op de hoogte werden gesteld door het NCSC over de Citrix-kwetsbaarheden op 13 januari 2020. Kan worden aangegeven waarom deze toezichthouders niet, net zoals de rijksoverheid en vitale aanbieders, zijn geïnformeerd op 9 januari 2020?
De aan het woord zijnde leden lezen voorts dat het NCSC op 16 januari 2020 op basis van informatie van specialisten beoordeelde dat de effectiviteit van de eerder uitgegeven tussentijdse mitigerende maatregelen onvoldoende zekerheid kon bieden. Kan worden toegelicht om welke mitigerende maatregelen het hier ging? Kan ook nader worden ingegaan op de onzekerheid van de effectiviteit van de maatregelen? Waren deze maatregelen bijvoorbeeld overgenomen uit Amerika of waren ze onafhankelijk opgesteld door het NCSC?
U beschrijft dat er op 16 januari 2020 nog altijd organisaties bleken te zijn die de tussentijdse mitigerende maatregelen van Citrix niet of in onvoldoende mate hadden genomen. Kan worden aangegeven in hoeverre het NCSC de dialoog is aangegaan met de betreffende organisaties om nader in te gaan op de beweegredenen achter het wel of niet uitvoeren van de mitigerende maatregelen?
Voornoemde leden constateren tevens dat meerdere keren in de brief wordt gesteld dat op verschillende momenten van genomen maatregelen de zekerheid van een sluitende oplossing voor de Citrix-kwetsbaarheden ontbrak. In het kader van landelijke coördinatie vragen zij in welke mate het NCSC verantwoordelijk was voor het zoeken naar een sluitende oplossing voor de kwetsbaarheden. In hoeverre waren andere betrokken organisaties binnen het Rijk hier verantwoordelijk voor?
Constaterende dat het mandaat van het NCSC zich beperkt tot het informeren van vitale aanbieders, vragen de aan het woord zijnde leden in hoeverre niet-vitale aanbieders (zoals het midden- en kleinbedrijf (MKB)) actief zijn geïnformeerd over de kwetsbaarheden van Citrix sinds 17 december 2019. Wanneer is het Digital Trust Center (DTC) bijvoorbeeld door het NCSC op de hoogte gesteld over de Citrix-kwetsbaarheden? In hoeverre is informatie gedeeld tussen het NCSC en het DTC tussen 17 december 2019 en het moment dat Citrix is afgesloten?
Naast vragen over de tijdlijn hebben de leden van de VVD-fractie ook vragen over de gekozen invalshoek voor de evaluatie en de toekomst van het gebruik van het Citrix-systeem. Relevante onderdelen zijn niet geëvalueerd, zo blijkt. Deelt u de mening dat alleen bij een volledige evaluatie lessen getrokken kunnen worden om in de toekomst te zorgen dat systemen en processen beter beveiligd zijn en dat bij lekken veel sneller, en wellicht adequater, gehandeld kan worden? Kunt u aangeven of het functioneren van de nationale crisisorganisatie en het NCSC geëvalueerd gaat worden? Zo ja, wanneer? Zo nee, waarom niet? Uit de voorliggende evaluatie is niet op te maken hoeveel organisaties zijn geraakt door het lek, waarom de rijksoverheid andere stappen nam dan andere organisaties en andere overheden en wat de impact van het

incident is geweest qua geleden schade. Wanneer kan de Kamer dit deel van evaluatie verwachten?
Wat betreft het toekomstige gebruik van het Citrix systeem van de rijksoverheid vragen voornoemde leden welke lessen zijn getrokken uit het Citrix-incident. Kunt u hier een overzicht van geven? Zo nee, waarom niet? Hoe veilig is de huidige manier waarop de rijksoverheid gebruik maakt van het Citrix-systeem?

De leden van de GroenLinks-fractie vragen wat de daadwerkelijke impact van het Citrix-incident was. Is een schatting gemaakt van de financiële en andere kosten? Zo nee, wordt daar nog aan gewerkt? Hoeveel organisaties en werknemers zijn geraakt door het Citrix-incident? In hoeverre is de veiligheid van vitale en niet-vitale processen in gevaar geweest? Met betrekking tot de nasleep van het Citrix-incident vragen deze leden voorts of al iets gezegd kan worden over de verantwoordelijkheid voor de kwetsbaarheid. Lag deze bij het bedrijf Citrix? Of bij kwaadwillende actoren die «exploits» ontwierpen? In hoeverre waren bedrijven en de overheid verzekerd tegen de geleden schade?
Voornoemde leden zijn verheugd met de snelle leerevaluatie van de gebeurtenissen rond de Citrix-kwetsbaarheid. Tegelijkertijd zijn zij verbaasd dat het functioneren van de nationale crisisorganisatie en van het NCSC niet tot de focus van de evaluatie behoorden. Wordt het algehele functioneren van het NCSC rond de Citrix-kwetsbaarheid alsnog apart geëvalueerd? Zo ja, wanneer kan de Kamer deze tegemoetzien? Zo nee, waarom niet?
Op 14 januari 2020 publiceerde het NCSC een bericht op de website waarin werd aangekondigd dat de kwetsbaarheid op dat moment qua ernst werd ingeschaald op een 9,8 op een schaal van 1 t/m 10.[1] De aan het woord zijnde leden vragen welke schaal hiervoor wordt gehanteerd. Zij zijn van mening dat 9,8 behoorlijk exact is en uitzonderlijk hoog en vragen dan ook waarom het dringende advies tot uitschakelen van Citrix-systemen pas drie dagen later kwam, op 17 januari 2020. Was inschaling van de ernst inmiddels ook verder opgelopen op de gehanteerde schaal? Zo ja, tot hoever?
De leden van de GroenLinks-fractie lezen in de snelle evaluatie dat bij veel organisaties vragen leefden over de verantwoordelijkheid van verschillende instanties binnen het Landelijk Dekkend Stelsel. Hoe kijkt u naar de kritiek van niet-vitale organisaties dat de verstrekking van specifieke informatie ten tijde van de Citrix-kwetsbaarheid tekortschoot? Kunt u daarbij ingaan op de rol van het DTC? Wat bent u van plan te ondernemen om het functioneren van het DTC bij toekomstige cyberincidenten te verbeteren? Hoe kijkt u naar de signalen dat voor veel organisaties niet duidelijk was wie de nationale regie voerde? Bent u bereid de rol van het NCSC bij digitale crisisbestrijding nog eens tegen het licht te houden en te bekijken of deze rol moet worden versterkt om effectief de nationale regie te kunnen voeren? Wat zijn de mogelijke gevolgen van meer nationale regie door de overheid voor de aansprakelijkheid?
Het WRR-rapport «Voorbereiden op digitale ontwrichting» benadrukt dat met digitale kwetsbaarheden geografische grenzen minder relevant worden. In de brief «Overzicht op hoofdlijnen Citrix-kwetsbaarheden» wordt echter geen melding gemaakt van overleg en afstemming met andere EU-lidstaten. In hoeverre is gedurende deze periode, en met name tijdens de kritieke week van 13 januari 2020, contact geweest met de cybersecuritydiensten van andere lidstaten en van de Europese Commissie om adviezen en maatregelen onderling af te stemmen? Wat verklaart de grote verschillen in maatregelen?

[1] https://www.ncsc.nl/actueel/nieuws/2020/januari/13/vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen

3. Kabinetsreactie op het rapport «Voorbereiden op digitale ontwrichting» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en een overzicht van de geleerde lessen van de Citrix-problematiek

De leden van de VVD-fractie lezen in uw brief dat het uitgangspunt is dat het NCSC, gebaseerd op dreigingsinformatie van de inlichtingen- en veiligheidsdiensten, zoveel mogelijk informatie deelt met partijen binnen het landelijk stelsel van cybersecurity. Kunt u aangeven in hoeverre vitale aanbieders door het NCSC worden geïnformeerd over «high end risks»? U stelt tevens in uw reactie dat het NCSC bepaalde vertrouwelijke informatie alleen deelt met aangewezen Computer Emergency Response Teams (CERTs) en Organisaties die *objectief kenbaar tot taak* hebben organisaties of het publiek te informeren over digitale kwetsbaarheden en dreigingen (OKTTs). Constaterende dat het DTC niet is aangemerkt als OKTT maar wel verantwoordelijk is voor het delen van informatie en verstrekken van informatie met 1,3 miljoen bedrijven, vragen deze leden waarom het DTC tot dusver nog niet is aangemerkt als OKTT. Bent u bereid voorwaarden te scheppen waardoor dit wel mogelijk is? Zo nee, waarom niet? Bent u bereid het functioneren van het DTC verder te onderzoeken en daarin mee te nemen hoe, gegeven de omvang van het DTC en het MKB, het DTC een vertrouwde positie kan innemen richting miljoenen ondernemers?
Overwegende dat grote, niet-vitale bedrijven niet behoren tot de doelgroep van het NCSC en het DTC, vragen voornoemde leden in hoeverre zij kunnen worden voorzien van voldoende specifieke informatie over digitale dreigingen door bijvoorbeeld een sectorale toezichthouder. Kan een overzicht worden gegeven welke sectoren wel en welke geen sectorale toezichthouder kennen?
De aan het woord zijnde leden constateren in de reactie op het WRR-rapport dat naar verwachting dit jaar nog een nieuw samenwerkingsplatform van politie, openbaar ministerie (OM), NCSC, Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) operationeel wordt. Zij vragen hoe dit samenwerkingsplatform zich zal verhouden tot het aangekondigde nationale responskader.
Tevens lezen de leden van de VVD-fractie dat u voornemens bent vitale aanbieders onder het volledige regime van de Wet beveiliging netwerk- en informatiesystemen (Wbni) te brengen via een te starten wetswijzigingstraject. Kan een overzicht worden gegeven van vitale aanbieders met zowel een meld- als zorgplicht en van vitale aanbieders met alleen een meldplicht?
Ook hebben voornoemde leden vragen over de vorderingen die dusver zijn gemaakt om het structurele digitale oefen- en stresstestenprogramma op te zetten conform de motie van het lid Weverling (Kamerstuk 24 095, nr. 496). Klopt het dat de digitale oefening ISIDOOR III wederom is uitgesteld, tot 2021? Kunt u toelichten hoe deze eenmalige, uitgestelde oefening zich verhoudt tot de Kamerbrede aangenomen motie van het lid Weverling die vraagt om een structureel digitaal oefen- en stresstestprogamma? Kunt u toelichten op welke termijn cross-sectorale cyberoefeningen zullen gaan plaatsvinden, naast de reeds geplande ISIDOOR-oefening, ter uitvoering van de motie van het lid Weverling? Is al contact gelegd met vitale partijen over het opstellen van een structurele oefenagenda? Zo nee, waarom niet?
Tot slot lezen de aan het woord zijnde leden dat de Cyber Security Raad de komende periode de brede aanpak van cybersecurity van de rijksoverheid zal gaan evalueren. Kunt u aangeven binnen welke termijn de Kamer de eerste voorlopige evaluatie kan verwachten? Kan ook worden aangegeven in hoeverre het onderzoek van de Cyber Security Raad zich verhoudt tot de inspanningen van het Ministerie van Binnenlandse Zaken

en Koninkrijksrelaties over informatieveiligheid naar aanleiding van de jaarlijkse rapporten van de Algemene Rekenkamer op Verantwoordingsdag?

De leden van de PVV-fractie lezen dat u op pagina 1 van uw brief schrijft: «De overheid moet zich daarom in samenwerking met private organisaties voorbereiden op incidenten in de digitale ruimte. Onze onverminderde inzet en investeringen blijven ook de komende jaren nodig om ons land digitaal veilig te houden.» Hoe gaat u dit doen?
Op pagina 2 lezen de aan het woord zijnde leden de volgende passage: «De WRR stelt dat het bestaande instrumentarium tijdens een crisis met digitale elementen moet worden aangepast en dat de overheid onvoldoende bevoegdheden heeft om in te grijpen. De WRR doet de aanbeveling om een helder afgebakende wettelijke bevoegdheid voor digitale hulptroepen te creëren en de noodzaak van een aparte regeling voor overheidshandelen gericht op tegengaan van escalatie te onderzoeken.» Voornoemde leden constateren dat u deze aanbeveling niet overneemt. Blijkbaar acht u het crisisplan en de evaluatie voldoende. Klopt dit? Zo ja, waar is dit standpunt op gebaseerd, ofwel waarom wordt deze aanbeveling niet overgenomen?
Op pagina 7 lezen de leden van de PVV-fractie bij het onderdeel «*Nationale respons»* de volgende passage: «Welke inzet aan de orde is, hangt af van de specifieke situatie en de verschillende belangen en afwegingen. Daarom wordt een geïntegreerd nationaal responskader opgesteld. Hierin maken de inlichtingen- en veiligheidsdiensten, politie, Defensie, BZ, OM, NCSC, betrokken vakdepartementen, veiligheidsregio's en de NCTV gezamenlijke werkafspraken over de respons bij een incident met digitale componenten. Dit responskader wordt de komende periode uitgewerkt en zal naar verwachting bij de eerstvolgende actualisering van het NCP-Digitaal operationeel zijn.» Wanneer is dat?
Op pagina 9 lezen de aan het woord zijnde leden bij het onderdeel «Wijziging Wet beveiliging netwerk- en informatiesystemen (Wbni)» de volgende passage: «Daartoe wil ik een wetswijzigingstraject starten zodat voor alle vitale aanbieders het volledige regime van de Wbni van toepassing wordt, voor zover sectorale wetgeving niet reeds dezelfde of strengere eisen stelt.» Wanneer wordt dat wetgevingstraject gestart?
Op pagina 13 lezen voornoemde leden de volgende passage: «Om onze digitale weerbaarheid te borgen zal de komende periode over de hele breedte meer geïnvesteerd moeten worden om de ontwikkelingen bij te kunnen houden. We zullen bovendien steeds kritisch moeten bekijken of het huidige instrumentarium en stelsel voldoende zijn.» Met betrekking tot deze passage hebben de aan het woord zijnde leden de volgende vragen. Kent u het opinieartikel «Het is tijd voor een Deltaplan Cybersecurity» van Bibi van den Berg en Inge Philips-Bryan, dat is verschenen in het Financieel Dagblad d.d. 13 september 2019? De leden van de PVV-fractie hebben jaren geleden al, onder verwijzing naar een artikel van Ronald Prins (https://www.emerce.nl/wire/ronald-prins-foxit-hebben-nieuwe-generatie-politici-nodig-voordat-thema-cybersecurity-goed-opgepakt) gepleit voor het overnemen van diens standpunt, inhoudende een soort deltacommissaris met een staf, voldoende budget en doorzettingsmacht.» Waarom laat u het aanpakken van cybergerelateerde problemen nog steeds over aan de betreffende vakministers waardoor een versnipperde aanpak bestaat hetgeen tot verwarring en overlapping van acties leidt? Wat vindt u van een Deltaplan Cybersecurity en het aanstellen van een Cybercommissaris, met het gezag en de middelen analoog aan de Deltacommissaris? Bent u bereid hier op zijn minst onderzoek naar te doen? Zo nee, waarom niet?

De leden van de CDA-fractie hebben kennisgenomen van uw brief van 20 maart 2020 waarin u aandacht besteedt aan geleerde lessen van de

Citrix-problematiek. Tevens hebben zij kennisgenomen van de antwoorden op eerder door hen gestelde Kamervragen ten aanzien van dit onderwerp. Mede naar aanleiding van een artikel op de website Techzine leidt dat tot nadere vragen bij voornoemde leden. In uw antwoorden op de Kamervragen lezen deze leden dat op 17 december 2019 de kwetsbaarheid bekend is gemaakt en dat er door Citrix per direct mitigerende maatregelen beschikbaar waren gesteld voor Citrix-producten, in afwachting van een patch die was voorzien voor eind januari 2020. Daarbij willen voornoemde leden aanstippen dat Citrix zelf heeft aangegeven dat het op juiste wijze en volledig doorvoeren van enkel de mitigatie voldoende was om het beveiligingslek (tijdelijk) te dichten. U geeft echter in de antwoorden op bovengenoemde vragen het volgende aan: «Of bij goed doorvoeren gebruikers beschermd waren tegen de kwetsbaarheid, hangt af van meer factoren dan alleen het al dan niet juist doorvoeren van deze maatregelen.» De aan het woord zijnde leden vragen u wat deze overige factoren zijn. Ook vragen zij of u bij het inzichtelijk maken van deze factoren per factor aan kunt geven hoe deze van toepassing was op het al dan niet beschermen van de Citrix-producten. Deelt u de mening dat indien de bewering van Citrix juist is, sprake is geweest van een onjuiste inschatting van de situatie door de Nederlandse overheid? Ook vragen de leden van de CDA-fractie of er geen aanleiding is juist de start van het Citrix-incident, de melding en het assessment van dat incident aan een nadere evaluatie te onderwerpen, inclusief de vraag welke betekenis kan en moet worden toegekend aan de termijn van 90 dagen waarbinnen een leverancier de tijd krijgt om een lek te herstellen. De aan het woord zijnde leden vragen of zij de rapportage van het COT juist hebben gelezen in die zin dat het COT naar de primaire waardering van het beveiligingsincident geen onderzoek heeft gedaan, maar deze als uitgangspunt heeft aangenomen. Ook willen deze leden weten hoe het komt dat het COT tot de waarneming «het advies niet afdoende was om het risico weg te nemen» komt. Kunt u, zo nodig vertrouwelijk, de Kamer informeren waar de inlichtingeninformatie die werd gebruikt voor de inschatting dat de kwetsbaarheid daadwerkelijk zou worden misbruikt en waarschijnlijk zelfs al werd misbruikt, uit bestond?

De leden van de CDA-fractie vragen welke maatregelen u denkt te nemen om juist in de diagnosefase van een groot cyberincident meer kennis en kunde in te bouwen. Kunt u uw antwoord formuleren in het licht van de één na laatste constatering in het COT-rapport waarin wordt gesteld dat het NCSC niet zelf in staat is om diepgaander technisch onderzoek uit te voeren en afhankelijk is van andere partijen? Ook vragen voornoemde leden welke andere partijen dit zijn.

Met betrekking tot het WRR-rapport «Voorbereiden op digitale ontwrichting» lezen de aan het woord zijnde leden dat één van de lessen die getrokken kan worden is dat het landelijk dekkend stelsel nog in opbouw is en «jong» is. Met name leeft er in de werkpraktijk nog onduidelijkheid over wat er dient te gebeuren in de «warme» fase als er daadwerkelijk problemen zijn en wat andere organisaties mogen verwachten van het NCSC, zo lezen voornoemde leden. Zij begrijpen uit de praktijk dat rondom de situatie met de Citrix-kwetsbaarheden de informatiedeling niet goed op orde was en dat het landelijk dekkend stelsel niet geheel dekkend was. Voornoemde leden vragen u of het NCSC vanuit de wettelijke grondslag enkel informatie over dreigingen en incidenten kan delen met CERTs en met OKTTs en dat bijvoorbeeld het DTC niet is aangewezen als een dergelijke OKTT en of dit als een beperkende factor gezien moet worden. Welke rol vervult het DTC als het gaat om cybersecurity?

De aan het woord zijnde leden vragen of u bereid bent een vertrouwenspersoon binnen de vitale sectoren aan te stellen, zodat de NCTV en het NCSC specifieke informatie over externe dreigingen, zoals statelijke actoren, kunnen delen en de sector zich gerichter kan beschermen. Kunt u

in overleg treden met de vitale sector en hen betrekken bij de versterkte aanpak binnen de Nationale Veiligheid Strategie?

De leden van de D66-fractie constateren dat de situatie rondom Pulse Secure en de Citrix- kwetsbaarheden twee kwetsbare elementen in het huidige cybersecuritybeleid blootlegden. Dit waren het mandaat op het gebied van informatiedeling door het NCSC en de mate waarin het doorvoeren van cruciale updates afgedwongen kan worden. Deelt u de mening dat deze twee elementen versterkt moeten worden om toekomstige situaties zoals Pulse Secure en Citrix beter het hoofd te kunnen bieden?
Op het gebied van informatiedeling hebben voornoemde leden al vaker aandacht gevraagd voor het mandaat van het NCSC, met name wat betreft het ontbreken van de mogelijkheid om informatie te delen met niet-vitale organisaties, alsmede het verrichten van scans om kwetsbare server te identificeren en informeren. Hoe staat het wat betreft het scannen van overheidssystemen in de vitale infrastructuur met de uitvoering van de motie van de leden Verhoeven en Laan-Geselschap (Kamerstuk 30 821, nr. 85)? Op het gebied van informatiedeling vragen de aan het woord zijnde leden u nader in te gaan op de mogelijkheid van het verbreden van het mandaat van het NCSC om relevante informatie (alle belangrijke beveiligingsinformatie (abuse informatie, gerichte actuele dreigingsinformatie, informatie over specifieke IP-adressen met kwetsbare systemen, etc.) ook te kunnen en mogen delen met Computer Emergency Response Teams (CERTs) van niet-vitale sectoren, inclusief CERTs die tot taak hebben om leveranciers van essentiële ICT-diensten te ondersteunen, en hen te ondersteunen en zorg te dragen voor een actieve benadering van die partijen met kwetsbare systemen, die niet door een CERT vertegenwoordigd worden. Bent u bereid het mandaat van het NCSC hiertoe te verbreden, en de knelpunten die dit in de weg staan weg te nemen? Zo ja, op welke manier?
De leden van de D66-fractie lezen in het WRR-rapport «Voorbereiden op digitale ontwrichting» dat Nederland onvoldoende is voorbereid. Wanneer kunt u zeggen dat Nederland wél voldoende is voorbereid? Welke indicatoren gebruikt u daarvoor? Beschikt u over voldoende middelen en bevoegdheden? Het WRR beveelt onder andere aan een cyberafhankelijkheidsbeeld te maken. Wat is de reden dat u dit bij sectorale toezichthouders wilt beleggen? Bent u bereid dit als onderdeel van het cybersecuritybeeld op te nemen? In de reactie op de aanbeveling van de WRR voor een Europese «cyberpool» schrijft u dat verzekeringen een belangrijke rol kunnen spelen bij digitale schade. Tegelijkertijd zien voornoemde leden dat verzekeringen ook qua cybersecurity een dubbele rol spelen, bijvoorbeeld bij het uitbetalen bij ransomware. Hoe kijkt u hier tegenaan? Is dit een wenselijke ontwikkeling? Leidt dit niet tot meer cybercriminaliteit?
De aan het woord zijnde leden vragen wanneer de Cyber Security Raad met haar evaluatie van de aanpak van cybersecurity en een advies over waar meer investeringen nodig zijn, naar aanleiding van de toezegging tijdens het algemeen overleg Cybersecurity op 30 oktober 2019 (op verzoek van het lid Verhoeven) om te bezien waar in de toekomst meer investeringen nodig zijn.

De leden van de GroenLinks-fractie zijn onder de indruk van het rapport «Voorbereiden op digitale ontwrichting» van de WRR en bedanken u voor de uitgebreide kabinetsreactie. Het rapport waarschuwt dat de bevoegdheden van de overheid bij een digitaal incident niet duidelijk zijn en dat organisaties en bedrijven de mogelijkheid hebben om digitale hulptroepen buiten de deur te houden, als zij dat in hun belang achten. In de kabinetsreactie zegt u toe dat u de wettelijke bevoegdheden van de overheid om in te grijpen bij digitale crises in kaart zal brengen. Wanneer

kan de Kamer deze verkenning tegemoetzien? Kunt u bij die verkenning ingaan op bevoegdheden in crisissituaties, maar ook bij digitale incidenten buiten grotere crisissituaties om, wanneer de nationale veiligheid als zodanig niet in het geding is? Kan de verkenning ingaan op bevoegdheden met betrekking tot zowel vitale als niet-vitale organisaties? Zal deze verkenning, tenslotte, ook een duidelijke reactie geven op de aanbeveling van de WRR om een helder afgebakende bevoegdheid voor digitale hulptroepen te creëren?
Voornoemde leden constateren dat het rapport benadrukt dat, in het digitale domein in het bijzonder, veel processen die raken aan de publieke taak zijn uitbesteed aan private partijen, veelal gevestigd in het buitenland. Dit creëert een afhankelijkheid van partijen waarover de overheid maar in beperkte mate invloed kan uitoefenen, ook in crisistijd. Deelt u deze analyse? Wat betekent dat voor onze capaciteit om risico's in het digitale domein te beheersen? De aan het woord zijnde leden verwelkomen de aanbeveling die de WRR doet tot het opstellen van een jaarlijks Cyberafhankelijkheidsbeeld om deze afhankelijkheden van buitenlandse partijen goed in kaart te brengen. Klopt het dat u deze aanbeveling niet overneemt omdat vitale aanbieders daar zelf voor verantwoordelijk zijn? Voornoemde leden zijn van mening dat digitale risico's het niveau van individuele aanbieders, of sectoren, overstijgen, gezien de sterke netwerkeffecten. Juist omdat de optelsom van individuele afhankelijkheden onvoldoende bekend is, volgens de WRR, is zo'n overkoepelend cyberafhankelijkheidsbeeld van groot belang, zo denken deze leden. Deelt u deze analyse? Bent u bereid deze aanbeveling op te volgen?
De leden van de GroenLinks-fractie constateren dat de WRR zich met betrekking tot de uitwisseling van informatie afvraagt of het huidige stelsel nog wel langs de juiste lijnen is ingericht en stelt dat die uitwisseling wordt belemmerd door het onderscheid tussen «vitale aanbieders» en «niet-vitale aanbieders». De WRR benadrukt dat ook het functioneren van niet-vitale toeleveranciers van grote invloed kan zijn op de continuïteit van vitale processen, en dat het maar de vraag is of het huidige onderscheid tussen vitale en niet-vitale aanbieders gehandhaafd moet blijven. Kunt u op deze stellingname reflecteren en hierbij ingaan op de vraag wat dit betekent voor de rolverdeling tussen het NCSC en DTC?
De WRR signaleert ook het ontbreken van een coherent beleid voor terugvalopties. De kabinetsreactie benadrukt juist dat organisaties zelf verantwoordelijk zijn voor hun eigen risicoanalyse en dat in het kader van die analyse ook gedacht kan worden aan terugvalopties. Voornoemde leden zijn benieuwd in hoeverre daar ook daadwerkelijk aan wordt gedacht en wat u onderneemt of van plan bent te ondernemen om u ervan te verzekeren dat inderdaad, op coherente wijze, aan terugvalopties wordt gedacht.
De aan het woord zijnde leden kunnen zich goed vinden in de aanbeveling van de WRR om meer aandacht te besteden aan het structureel oefenen op digitale crisissituaties. Klopt het dat ISIDOOR III wederom is uitgesteld, nu tot 2021? Wanneer wordt gestart met een structureel oefenprogramma tussen de overheid en vitale aanbieders?

De leden van de SP-fractie vonden het redelijk ontluisterend om in het WRR-rapport te lezen dat voor de omgang met incidenten in de fysieke wereld een uitgebreide crisisorganisatie en allerlei voorzieningen en wettelijke regels bestaan, maar dat deze zaken grotendeels ontbreken voor incidenten in de digitale wereld. Heeft de overheid niet achter de feiten aangelopen? Waarom heeft de regering dit WRR-rapport nodig gehad om in actie te komen? De WRR wijst er in haar rapport op dat (geopolitieke) cyberaanvallen niet zijn te voorkomen, maar dat de vraag vooral is wat ertegen te doen valt. Toch zijn bijna alle maatregelen die

door de regering tot nu toe zijn genomen juist gericht op preventie. Hoe verklaart u dat?
De aan het woord zijnde leden constateren dat de afgelopen decennia veel publieke voorzieningen in private handen zijn gekomen en dat de overheid de digitale ondersteuning van haar activiteiten heeft uitbesteed aan softwareleveranciers en digitale dienstverleners. Deelt u de mening dat de continuïteit van de samenleving hierdoor sterk afhankelijk is geworden van het doen en laten van private partijen, die in veel gevallen vanuit het buitenland opereren? Wat vindt u daarvan? Is deze afhankelijkheid, zeker in gevallen van crisis, niet te groot? Kunt u hier eens uitgebreid op reflecteren?
De leden van de SP-fractie vragen of het niet beter zou zijn als de Nederlandse overheid zelf veel meer regie houdt over belangrijke digitale infrastructuren, bijvoorbeeld door de ontwikkeling van nieuwe software of digitale diensten binnen de Nederlandse grenzen te houden, zodat de Nederlandse toezichthouders kunnen toezien of de Nederlandse (digitale) samenleving wel voldoende wordt beschermd in geval van crisis? Zo nee, kunt u uitgebreid motiveren waarom niet? Waarom laat u de verantwoordelijkheid bij individuele vitale aanbieders voor de beveiliging van vitale digitale infrastructuren? Als de veiligheid van de samenleving in het geding is, dan is dit toch juist een taak voor de overheid om goed te regelen?
De aan het woord zijnde leden vragen wat u vindt van de mogelijkheid om in ieder geval de overheid zelf en bedrijven in de vitale sectoren te verplichten een analoog of digitaal back-upsysteem te hebben waarop ze kunnen terugvallen, dat niet is verbinding staat met andere bronnen en dus op zichzelf kan functioneren, in het geval dat sprake is van een cyberaanval dan wel storing op het primaire netwerk? Kunt u uitgebreid motiveren waarom u hier wel of niet iets in ziet?
Voornoemde leden constateren dat het WRR-rapport spreekt van «digitale hulptroepen» die zouden moeten helpen bij de bestrijding van digitale verstoringen die een maatschappelijk ontwrichtend effect kunnen hebben. Hoe zien deze hulptroepen er volgens u uit? Is dat het NCSC? Heeft het NCSC voldoende kennis en mensen in huis om die zogenaamde hulptroepen te vormen als dat nodig is of moet deze expertise telkens ingehuurd worden? Mocht dat laatste het geval zijn, wordt die expertise dan in Nederland gezocht of ook buiten de landsgrenzen?

4. Cybersecurity en corona

De leden van de VVD-fractie willen stilstaan bij de signalen die hen bereiken over nieuwe vormen van cybercrime en een voorziene toename van digitale aanvallen. Cybercriminelen die de huidige crisis rondom corona aangrijpen om bijvoorbeeld thuiswerkers te hacken, ziekenhuissystemen te ondermijnen of CEO-fraude te plegen (waarbij een financieel medewerker een dringende mail krijgt die afkomstig lijkt te zijn van de directeur waarin gevraagd wordt om direct een bepaald bedrag over te maken). Voornoemde leden willen ook stilstaan bij veilig digitaal thuiswerken. Welke ontwikkelingen ziet u? Hoe wordt dit gemonitord en op welke wijze zijn onze veiligheidsdiensten voorbereid om hierbij snel op te treden? Kunt u daarbij aangeven op welke wijze in internationaal verband wordt samengewerkt en hoe informatie wordt gedeeld om te voorkomen dat criminelen op grote schaal misbruik maken van de huidige crisis? Welke concrete maatregelen worden in internationaal verband genomen om de uitwisseling van informatie te bevorderen?

De leden van de CDA-fractie herkennen hoe in deze tijd van thuiswerken en videoconference de integriteit en stabiliteit van het internet van essentieel belang is. Welke inspanningen worden geleverd door het cybersecuritystelsel van de Nederlandse overheid, onder aanvoering van

het NCSC, om te monitoren en juist in deze tijd extra te bevorderen dat ons internet stabiel en veilig blijft, zeker richting essentiële organisaties als ziekenhuizen, verpleeghuizen, huisartsen en alle andere vitale plekken in de zorg? Daarbij vragen deze leden of u bij deze vraag ook de urgentieverklaring van de Cyber Security Raad van 31 maart 2020 wilt betrekken.
De aan het woord zijnde leden vragen of u kennis heeft genomen van de uitzending van Reporter Radio (d.d. 5 april 2020) waarin gerapporteerd werd, op basis van onderzoek van TNO, dat er in één week tienduizend nieuwe domeinnamen bij kwamen die gelinkt konden worden aan COVID-19? Ook vragen zij naar uw reactie op de conclusie dat ongeveer de helft van de bedrijven op die lijst niet te vertrouwen is en zich waarschijnlijk bezighoudt met phishing. Welke mogelijkheden ziet u voor de Nederlandse overheid om actief te werken aan het uit de lucht halen van dergelijke websites?
Voornoemde leden vragen of u bekend bent met initiatieven vanuit het private veld om de overheid juist in deze coronatijd belangeloos te ondersteunen, zoals bijvoorbeeld Tech Tegen Corona. Daarbij vragen zij of, zeker als het gaat om cybersecurity, door uw ministerie actief gebruik gemaakt van dit aanbod.
Welke vormen van videoconferencing worden door u naar de huidige standaarden gezien als veilig en betrouwbaar, zeker voor gebruik door de Nederlandse overheid? Ook vragen de aan het woord zijnde leden of u bereid bent op korte termijn een waardering voor de veelgebruikte applicaties te geven, dan wel een onafhankelijke organisatie in het veld te vragen hier een onderzoek naar te doen. De aan het woord zijnde leden vragen naar de mogelijkheden die u als coördinerend bewindspersoon voor cybersecurity en crisisbeheersing heeft om richtinggevende uitspraken te doen naar overheidsorganen (landelijk, decentraal) om bepaalde (onveilige) videoconferencesystemen of -applicaties niet te gebruiken.

De leden van de D66-fractie constateren dat cybersecurity hand in hand gaat met een steeds verder digitaliserende samenleving. Die ontwikkeling was al gaande vóór de huidige coronacrisis en die ontwikkeling wordt nu op veel gebieden verder versneld. Neem al die mensen die nu thuiswerken, thuis onderwijs volgen of digitale dokterconsulten voeren. De impact van de Citrix-kwetsbaarheid van begin dit jaar zou enkele maanden later nog veel grotere maatschappelijke en economische gevolgen hebben. Voornoemde leden menen daarom dat de urgentie van goed cybersecuritybeleid verder is toegenomen door de coronacrisis. Deelt u deze mening? Welke gevolgen op het gebied van cybersecurity ziet u als gevolg van de coronacrisis? Bent u van mening dat de coronacrisis noopt tot heroverweging van de aanwijzing van wat «essentiële diensten» zijn in het kader van de Wbni, bijvoorbeeld als het gaat om hosting- of datacenters?

De leden van de GroenLinks-fractie signaleren toenemende risico's voor de cybersecurity als gevolg van de coronacrisis. Het lijkt erop dat onder meer door het grootschalige thuiswerken cybercriminelen vaker kans zien om in de digitale infrastructuur van bedrijven, overheden en organisaties binnen te dringen. Kan een beeld worden gegeven van het huidige cyberdreigingsniveau en hoeveel incidenten zich tot nu toe hebben voorgedaan? Welke specifieke bedreigingen voor de cybersecurity vragen momenteel extra aandacht en hoe worden deze extra bedreigingen precies het hoofd geboden? Is er voldoende capaciteit en expertise voorhanden om te voorzien in een adequaat handhavingsniveau?
Voornoemde leden hebben kennisgenomen van een groot aantal initiatieven en samenwerkingsverbanden om met name de zorg te ondersteunen in het waarborgen van de continuïteit van hun werkzaamheden. Zo werkt het NCSC samen met Z-CERT en is er het initiatief van

cybersecuritydeskundigen uit ruim veertig landen die onder de naam COVID-19 CTI League samenwerken in de strijd tegen uiteenlopende vormen van cybercriminaliteit. De deelnemende deskundigen proberen beschikbare informatie en expertise te delen, om zo bijvoorbeeld phishingcampagnes vroegtijdig op te sporen en om aan de hand van signalen te voorspellen welke ziekenhuizen doelwit kunnen worden van een cyberaanval. Ook andere initiatiefnemers bieden overheden, hulpverleners, zorgverleners en ziekenhuizen kosteloos of tegen gereduceerd tarief cybersecurity-expertise aan om in de breedste zin een bijdrage te leveren aan de strijd tegen het coronavirus. Wat vindt u van deze samenwerkingsvormen? Hoe houdt u zicht op deze ontwikkelingen en welke lessen kunnen hieruit worden geleerd om de beveiliging tegen cybercrime op een hoger plan te tillen? Hoe verloopt precies de coördinatie van en samenwerking tussen alle betrokken diensten, overheden, organisaties en bedrijven in de strijd tegen cyberaanvallen in coronatijd? Welke kansen en risico's ziet u in de samenwerking op cybersecurity tussen publieke en private organisaties?
Juist onder deze buitengewone omstandigheden moet naar het oordeel van de aan het woord zijnde leden maximaal worden ingezet op veiligheid van de ICT-systemen en op de betrouwbaarheid van verbindingen en berichtgeving via internet en sociale media. Voornoemde leden vragen in dat verband welke stappen bijvoorbeeld zijn ondernomen tegen nep-RIVM-websites en tegen malware-aanvallen tegen ziekenhuizen die de afgelopen periode actief zijn geweest. Daarnaast zijn deze leden benieuwd hoe u heeft bijgedragen aan de veiligheid en de beveiliging van thuiswerkers met cruciale beroepen.

De leden van de ChristenUnie-fractie zijn van mening dat juist in de coronacrisis het belang van digitale veiligheid, dataveiligheid en stabiele netwerken zichtbaar wordt. Hierbij heeft de overheid wat deze leden betreft een voorbeeldrol te vervullen. Juist in tijden van crisis dient de overheid het belang van privacy in het oog te houden. Voornoemde leden volgen dan ook nauwgezet het proces om te komen tot zogeheten Corona-apps. Uitgangspunten van deze leden hierbij zijn in ieder geval:
– Vrijwillige deelname,
– Tijdelijkheid,
– Decentrale opslag van data,
– Geanonimiseerd,
– Open source,
– In lijn met privacywetgeving,
– Naast samenwerking met commerciële partijen ook de academische wereld betrekken.

Met instemming constateren de leden van de ChristenUnie-fractie dat in de brief «COVID-19 Update stand van zaken» (Kamerstuk 25 295, nr. 249) een groot aantal van deze uitgangspunten als eis is geformuleerd door het kabinet. Graag krijgen deze leden een toelichting of niet ook vrijwillige deelname een eis behoort te zijn. Tevens vragen zij of naast commerciële partijen ook universiteiten en academische instellingen bij de uitwerking worden betrokken. Voorts vragen de aan het woord zijnde leden of de Data protection impact assessment van de uiteindelijke applicaties openbaar zullen zijn, ten behoeve van maatschappelijk vertrouwen.
Een serieus punt van zorg voor de leden van de ChristenUnie-fractie is de cybersecurity in de zorgsector. Op welke wijze vindt hierin coördinatie plaats met zorgpartijen en is hierin ook oog voor kleinere zorginstellingen? Voornoemde leden zijn zeer positief over het initiatief wijhelpenziekenhuizen.nl waarbij bedrijven zorginstellingen helpen op het gebied van cybersecurity. Welke mogelijkheden ziet u om zorginstellingen ook nadrukkelijk op dit initiatief te wijzen?
De aan het woord zijnde leden lezen met zorg recente berichten over de vernieling van zendmasten uit angst voor vermeende gezondheidsef-

fecten en 5G. Welk risico brengt dit met zich mee voor de netwerkcapaciteit, juist ook nu veel vanuit huis wordt gewerkt en gebruik wordt gemaakt van videobellen en videodiensten? Kan, gezien het feit dat het hier een onderdeel van de kritische nationale infrastructuur betreft, worden aangegeven wat de gevolgen zijn voor de nationale veiligheid? Is er aanleiding beveiliging op te schalen, om zo leveringszekerheid te kunnen borgen? Bent u ook bereid om sociale media platforms aan te spreken op hun verantwoordelijkheid om valse berichtgeving tegen te gaan die aan kan zetten tot deze daden van brandstichting? Wordt samengewerkt met andere overheden, waaronder het Verenigd Koninkrijk, om verspreiding van complottheorieën tegen te gaan?
De leden van de ChristenUnie-fractie vragen of een toename zichtbaar is op het gebied van cybercriminaliteit. Hoe kunnen burgers worden geholpen om in deze tijd, waarin veel contact, handelingen en ook privacygevoelig verkeer zich online afspeelt, ook op gebieden en/of met een intensiteit waarvoor dat voorheen niet gebruikelijk was, zich veilig in de digitale wereld te bewegen?
Ten aanzien van cybercriminaliteit vragen de aan het woord zijnde leden voorts welke ontwikkelingen zichtbaar zijn in gedwongen prostitutie via het darkweb en apps als telegram. Wat is de stand van zaken in de opsporing? Hoe vaak is het afgelopen jaar gebruik gemaakt van de webcrawler? Wordt, sinds de afkondiging van een verbod op contactberoepen en de sluiting van seksinrichtingen, een toename geconstateerd van prostitutieadvertenties op genoemde kanalen? Wordt daar vervolgens ook op gehandhaafd?

5. Overig

De leden van de CDA-fractie zijn verheugd over de extra inspanningen voor onderzoek en innovatie op het gebied van cybersecurity (ruim 20 miljoen euro) voor onderzoek en innovatie op het gebied van cybersecurity (zie de brief «Resultaten verkenningen en vervolgaanpak cybersecurity kennisontwikkeling en innovatie» (Kamerstuk 26 643, nr. 674) van de Staatssecretaris van Economische Zaken en Klimaat) maar vragen tegelijkertijd hoe die inspanningen zich verhouden tot investeringen in andere landen. Kunt u aangeven welke soortgelijke investeringen in landen als Duitsland en Frankrijk worden gedaan? Denkt u dat de Nederlandse investering voldoende is om toptalent en topkennis aan ons land te binden? Ook vragen deze leden of bij het antwoord op deze vragen de constatering van TNO dat de totale onderzoekscapaciteit in Nederland op het vlak van cybersecurity bescheiden is.

II. Reactie van de Minister van Justitie en Veiligheid

1. Inleiding

Ik dank de leden van de vaste commissie voor Justitie en Veiligheid voor hun opmerkingen en vragen over de brieven inzake «Overzicht op hoofdlijnen Citrix-kwetsbaarheden» (Kamerstuk 26 643, nr. 660), «Analyse van de gelopen risico's door de kwetsbaarheden in de virtual private network (VPN) software van het bedrijf Pulse Secure» (Kamerstuk 26 643, nr. 666), «Verzoek aan de commissie over het aanhouden van een verslag van schriftelijk overleg over het overzicht op hoofdlijnen Citrix-kwetsbaarheden» (Kamerstuk 26 643, nr. 667), «Kabinetsreactie op het rapport «Voorbereiden op digitale ontwrichting» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en een overzicht van de geleerde lessen van de Citrix-problematiek» (Kamerstukken 26 643 en 30 821, nr. 673). Hieronder beantwoord ik de gestelde vragen. Voor het Zomerreces ontvangt uw Kamer nog een brief met een beleidsreactie op het Cyber Security Beeld Nederland (CSBN2020) en de voortgangsrapportage van

de Nederlandse Cyber Security Agenda (NCSA) naar aanleiding van deze brief en de hierboven genoemde brieven ga ik op een later moment graag nog eens met uw Kamer in gesprek.

2. Overzicht op hoofdlijnen Citrix-kwetsbaarheden

De leden van de VVD-fractie vragen naar de periode tussen het bekend worden van de kwetsbaarheid op 17 december en het actief publiekelijk informeren van vitaal aanbieders op 9 januari. Een gedetailleerde tijdslijn van gebeurtenissen heb ik met uw Kamer gedeeld per brief van 23 januari[2] en via de technische briefing aan uw Kamer op diezelfde dag. De VVD-fractie stelt dat het Nationaal Cybersecurity Centrum (NCSC) pas vanaf 9 januari 2020 vitale gebruikers van de betreffende Citrix producten (Citrix-ADC en Citrix-Gateway) actief publiekelijk geïnformeerd heeft over de kwetsbaarheid. Het NCSC heeft echter al op 18 december 2019 een eerste beveiligingsadvies over deze kwetsbaarheid gepubliceerd en actief gedeeld met haar doelgroepen, waaronder organisaties in de vitale infrastructuur. In de dagen en weken daaropvolgend is – wanneer daar aanleiding toe was – het advies door het NCSC geactualiseerd. Het advies waarover de VVD-fractie spreekt betreft dus het geactualiseerde advies dat is gebaseerd op eerdere actief gedeelde adviezen van het NCSC hierover. De aanleiding voor het actualiseren van het advies op 9 januari 2020 was de verwachting dat er op korte termijn een zogeheten *exploitcode* publiekelijk bekend zou worden waarmee de kwetsbaarheid kon worden misbruikt. Tevens werd bekend dat er actief werd gezocht naar kwetsbare systemen, potentieel door kwaadwillende. **De hierboven genoemde leden vragen mij ook welke concrete maatregelen naast het informeren van vitale aanbieders door het NCSC zijn genomen tussen het publiekelijk informeren over de kwetsbaarheden op 9 januari 2020 en het advies met betrekking tot het afsluiten van het Citrix systeem uitgegeven op 17 januari 2020**. Ik verwijs u naar het gedetailleerde overzicht dat ik hierover heb gedeeld per brief van 23 januari[3] en per technische briefing aan uw Kamer op diezelfde dag. **De leden van de VVD-fractie vragen naar het te volgen protocol in geval van een lek in het betreffende Citrix-systeem.** Het NCSC publiceert honderden adviezen per jaar over kwetsbaarheden. Er bestaat daarom niet voor elke afzonderlijke leverancier een apart protocol voor opvolging bij kwetsbaarheden. In het algemeen geldt dat het NCSC aan de hand van een inschalingsmatrix adviezen inschaalt op ernst en een advies opstelt hoe om te gaan met de kwetsbaarheid. Het is van belang dat vitale aanbieders zelf in beeld hebben welke software zij gebruiken en daaropvolgend een risico-inschatting maken bij kwetsbaarheden in deze software. Daarnaast werk ik samen met vitale aanbieders, sectorale toezichthouders en vakdepartementen aan een methodiek van »pas toe of leg uit» bij ernstige beveiligingsadviezen, in deze gevallen zullen toezichthouders actief nagaan of adviezen zijn opgevolgd door vitale aanbieders of dat er een goede reden is om dit niet te doen. Voor alle overheidslagen geldt daarnaast de verplichte maatregel: als de kans op misbruik en de kans op schade bij misbruik beiden hoog zijn, worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen[4]. Daarnaast geldt voor de rijksoverheid een meldplicht (binnen 72 uur) aan het NCSC bij geconstateerde inbreuken[5]; de andere bestuurslagen hebben een meldplicht bij hun sectorale

---

[2] Kamerstuk 26 643, nr. 660
[3] Kamerstuk 26 643, nr. 660
[4] BIO 12.6.1.1
[5] BIO 16.1.4.1

Computer emergency response team (CERT). Ik blijf tenslotte de oproep doen om beveiligingsadviezen van het NCSC zo snel als mogelijk op te volgen en zodoende kans op misbruik te voorkomen. **De VVD-fractie vraagt ook of kan worden aangegeven waarom de sectorale toezichthouders niet zijn geïnformeerd op 9 januari 2020 in plaats van 13 januari**. De eerste prioriteit van het NCSC is het waarschuwen van doelgroep-organisaties die de betreffende systemen gebruiken waarin kwetsbaarheden zijn geconstateerd. Zij zijn namelijk degenen die als eerste actie moeten ondernemen om misbruik van de kwetsbaarheden te voorkomen. Ik ben het met de leden van de VVD-fractie eens dat het tijdig delen van dreigingsinformatie met de toezichthouders van vitale aanbieders van groot belang is. Zij hebben een belangrijke rol in het stelsel en kunnen organisaties er in het kader van hun toezichthoudende taken op wijzen dat zij nog kwetsbaar zijn en dat zij de nodige beveiligingsmaatregelen moeten treffen. Om de positie van de toezichthouders te versterken kondigde ik in mijn brief van 29 oktober 2019 aan dat het NCSC meer informatie met toezichthouders zal uitwisselen[6]. Het rechtstreeks informeren van de toezichthouders over de Citrix-kwetsbaarheid is een goed voorbeeld van deze intensievere samenwerking. Er wordt ondertussen verder gewerkt aan het binnen de wettelijke kaders nader inrichten van de informatiedeling en overige samenwerking tussen NCSC en sectorale toezichthouders, waarbij de snelheid van informatiedeling ook als factor wordt meegewogen. Hierdoor zullen toezichthouders waar mogelijk voor hen relevante dreigingsinformatie van het NCSC ontvangen.

De leden van de VVD-fractie vragen vervolgens in hoeverre de rijksoverheid en vitale aanbieders die gebruik maken van de betreffende Citrix software risico hebben gelopen. De leden van de GL-fractie vragen daarnaast ook in hoeverre de veiligheid van niet-vitale processen in gevaar is geweest door Citrix. De AIVD en MIVD bevestigden destijds dat een statelijke actor de kwetsbaarheid in Citrix-servers gebruikte bij voorbereidingen op cyberspionage. Een groot deel van de rijksoverheid en de vitale aanbieders hebben de beveiligingsadviezen van het NCSC tijdig opgevolgd. CIO Rijk hield daarbij voor de rijksoverheid een overzicht bij van organisaties die de betreffende Citrix-software hadden afgeschakeld of – als dat niet was gebeurd – welke mitigerende maatregelen zij namen en wat de impact daarvan was. Het beeld is dat de gevolgen – anders dan enkele dagen problemen met het werken op afstand – voor de rijksoverheid beperkt zijn gebleven. Voor de vitale aanbieders komt dit beeld overeen. Voor wat betreft niet-vitale aanbieders zijn mij bijvoorbeeld uit de media signalen bekend dat er pogingen tot misbruik zijn geweest bij niet vitale organisaties. **De leden van de VVD-fractie benoemen dat het NCSC op 16 januari 2020 op basis van informatie van specialisten beoordeelde dat de effectiviteit van de eerder uitgegeven tussentijdse mitigerende maatregelen onvoldoende zekerheid konden bieden. Zij vragen om welke mitigerende maatregelen het ging.** Het betrof de mitigerende maatregelen die door Citrix zelf werden gepubliceerd tot een sluitende oplossing beschikbaar zou zijn. Het NCSC heeft in dat kader op 16 januari bij zijn doelgroepen aangegeven dat het onduidelijk was of de tussentijdse mitigerende maatregelen van Citrix in alle gevallen effectief zouden zijn voor het voorkomen van misbruik. Daarop heeft het NCSC zelf aanvullende beveiligingsmaatregelen aanbevolen, waaronder IP-whitelisting en het instellen van een zogeheten webapplicatiefirewall. Naast deze aanvullende beveiligingsmaatregelen heeft het NCSC geadviseerd te overwegen om systemen met de betreffende Citrixproducten uit te schakelen of waar mogelijk de aanvullende maatregelen te

[6] Kamerstuk 26 643, nr. 647

treffen[7]. **De leden van de CDA-fractie vragen mij vervolgens naar de juistheid van de inschatting door de Nederlandse overheid over de effectiviteit van de door Citrix zelf afgekondigde mitigerende maatregelen.** Daarover kan ik u vertellen dat mede op basis van technisch onderzoek het NCSC beoordeelde dat de effectiviteit van de tussentijdse mitigerende maatregelen van Citrix onvoldoende zekerheid konden bieden. Ik blijf daarom achter het gevoerde beleid staan rondom de Nederlandse aanpak van de kwetsbaarheid in Citrix-ADC en Citrix-Gateway. **De leden van de CDA-fractie vragen mij ook naar de overige factoren – naast het juist doorvoeren van de mitigerende maatregelen van Citrix – die van toepassing waren op de bescherming van de gebruikers tegen deze kwetsbaarheid.** Het NCSC is tot het advies van 16 januari 2020 – om waar nodig de kwetsbare Citrix-systemen uit te schakelen -gekomen op basis van onduidelijkheid over de effectiviteit van de maatregelen die door Citrix waren gepubliceerd.[8] De hierop volgende adviezen van het NCSC over hoe verder te handelen hadden mede te maken met de tijdigheid waarin organisaties de mitigerende maatregelen hadden getroffen, welke versies in gebruik waren en was tevens afhankelijk van de dreiging die uitging naar deze organisaties. **De leden van de VVD-fractie vragen of kan worden aangegeven in hoeverre het NCSC de dialoog is aangegaan met de betreffende organisaties om nader in te gaan op de beweegredenen achter het wel of niet uitvoeren van de mitigerende maatregelen.** Ik benadruk dat deze risicoafweging in de eerste plaats door organisaties zelf moet worden gemaakt omdat zij kunnen bepalen of het wel of niet doorvoeren van beveiligingsmaatregelen impact kan hebben op de veiligheid en op de continuïteit van de bedrijfsvoering van deze organisaties. Het wel of niet doorvoeren van maatregelen vergt namelijk uitvoerige kennis van de veelal complexe digitale infrastructuur van deze organisaties. Ik kan u melden dat het NCSC voortdurend in contact staat met zijn doelgroepen (rijksoverheid en Vitaal). Uit de Citrixevaluatie blijkt dat er nog enkele verbeterpunten zijn. Hier ga ik de komende tijd mee aan te slag. Deze lessen worden o.a. meegenomen bij het opstellen van de handreiking Landelijk Dekkend Stelsel en het responskader bij digitale incidenten.

De leden van de VVD-fractie willen weten in welke mate het NCSC, of andere organisaties binnen de rijksoverheid, verantwoordelijk zijn voor het zoeken naar een sluitende oplossing voor de kwetsbaarheden. De kwaliteit van een product is allereerst de verantwoordelijkheid van de leverancier. Dat geldt dus ook voor softwareleveranciers. Zij zijn het beste in staat om de benodigde beveiligingsupdates te ontwikkelen voor hun eigen product indien daar kwetsbaarheden in worden gesignaleerd. Het NCSC kan daartoe een rol spelen door informatie over kwetsbaarheden, die mede naar aanleiding van meldingen in het kader van Coordinated Vulnerability Disclosure (CVD) is verkregen met leveranciers te delen. Daarnaast werkt mijn collega van het Ministerie van EZK aan de uitvoering van de «Roadmap Digitaal Veilige Hard- en Software». Deze Roadmap biedt een samenhangend pakket aan maatregelen om onveiligheden in hard- en software te voorkomen, kwetsbaarheden op te sporen en om de gevolgen daarvan te mitigeren. Naast aanbieders van digitale producten en diensten hebben gebruikers (overheden, bedrijven en consumenten) een eigen verantwoordelijkheid om de vraag naar digitaal veilige producten en diensten te stimuleren en een risico-afweging te maken welke producten en diensten zij gebruiken.

---

[7] Zie https://www.ncsc.nl/actueel/nieuws/2020/januari/16/door-citrix-geadviseerde-mitigerende-maatregelen-niet-altijd-effectief

[8] Zie https://www.ncsc.nl/actueel/nieuws/2020/januari/16/door-citrix-geadviseerde-mitigerende-maatregelen-niet-altijd-effectief

De leden van de VVD-fractie vragen wanneer het Digital Trust Center (DTC) op de hoogte is gesteld over de Citrix kwetsbaarheden door het NCSC. Ook vragen zij in hoeverre er informatie is gedeeld tussen het NCSC en het DTC en in hoeverre niet-vitale aanbieders actief geïnformeerd zijn over de Citrix kwetsbaarheden. Citrix maakte op 17 december 2019 bekend dat er sprake was van een kwetsbaarheid in de genoemde Citrix producten. Het NCSC heeft daarom op 18 december 2019 een eerste beveiligingsadvies voor deze kwetsbaarheid gepubliceerd. In de daaropvolgende periode zijn deze adviezen meerdere keren geactualiseerd. Daarbij heeft het NCSC uiteraard doorlopend samenwerkingspartners, zoals het DTC, zoveel als mogelijk geïnformeerd over de ontwikkelingen, zodat zij hun eigen doelgroep actief konden benaderen. Het DTC heeft vrijwel direct na het bekend worden van opschaling van deze kwetsbaarheid op 24 december continu actuele informatie over de kwetsbaarheid aan haar doelgroep van niet-vitale bedrijven gestuurd. Het heeft hiertoe al zijn kanalen ingezet: nieuwsberichten op de website, sociale media en e-mails aan de samenwerkingsverbanden van bedrijven. Al deze berichten zijn gebaseerd op de berichten van het NCSC inclusief de duiding en het geboden handelingsperspectief. Tevens heeft het DTC daar waar noodzakelijk input geleverd voor de diverse (interdepartementale) crisisberaden. **De leden van de GL-fractie vragen hoe de Minister aankijkt tegen de kritiek van niet-vitale organisaties dat de verstrekking van specifieke informatie ten tijde van de Citrix-kwetsbaarheid tekortschoot. Deze leden vragen om in te gaan op de rol van het Digital Trust Centre (DTC)**. Zowel het NCSC als het DTC hebben actief gecommuniceerd over de Citrix-kwetsbaarheid via diverse kanalen. In beginsel zijn organisaties, binnen de (Rijks)overheid, de vitale infrastructuur en daarbuiten, zelf verantwoordelijk voor de beveiliging van hun digitale systemen en het verhelpen van kwetsbaarheden binnen die systemen. De adviezen van het NCSC en het DTC zijn bedoeld om deze organisaties hiertoe in staat te stellen. Voortdurend wordt gekeken op welke wijze informatie beter en sneller gedeeld kan worden: zowel tussen de overheid en het bedrijfsleven als tussen organisaties onderling. Het kabinet werkt toe naar een Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden. Dit stelsel is echter nog in ontwikkeling, de gesignaleerde verbeterpunten worden hierin meegenomen. **De leden van de GL-fractie willen weten wat het kabinet van plan is om het functioneren van het DTC bij toekomstige cyberincidenten te verbeteren**. Momenteel wordt er door het Ministerie van EZK gewerkt aan het laten voldoen van het DTC aan de wettelijke voorwaarden waardoor het DTC aangewezen kan worden als een organisatie die objectief kenbaar tot taak heeft andere organisaties of het publiek te informeren (OKTT). In geval van een dergelijke aanwijzing kan het NCSC ook persoonsgegevens in relatie tot informatie over digitale kwetsbaarheden en dreigingen (bv. IP-adressen), die het NCSC als bijvangst van de reguliere taakuitoefening ten behoeve van Rijk en vitaal heeft verkregen, voor zover relevant voor de taakuitoefening van het DTC, delen met het DTC. Daarnaast zal er praktische invulling worden gegeven aan de samenwerkingsafspraken tussen DTC en NCSC, teneinde het DTC bij cyberincidenten voor zover mogelijk door het NCSC nog gerichter van voor het niet-vitale bedrijfsleven relevant handelingsperspectief te voorzien.

Vanuit de fracties VVD, CDA en GL zijn vragen gesteld die ingaan op de scope van de evaluatie die door COT is uitgevoerd naar aanleiding van de problematiek rondom Citrix in januari 2020. De samenvatting van deze evaluatie is met uw Kamer gedeeld per brief van

20 maart[9]. Ik kan u allereerst toelichten dat de scope van de evaluatie de werking van het gehele stelsel is geweest. De evaluatie van de samenwerking in het gehele stelsel – het Landelijk Dekkend Stelsel – biedt juist relevante inzichten om de digitale weerbaarheid te verhogen. De focus op één actor zou een te beperkte scope zijn om interessante inzichten te signaleren. Om die reden zijn er door het Instituut voor Veiligheids- en Crisismanagement (COT) diverse lessensessies opgezet samen met de partners uit het Landelijk Dekkend Stelsel, waaronder sectorale computercrisisteams, vitale aanbieders, NCSC en CIO-Rijk. Uit deze evaluatie kunnen wat mij betreft waardevolle lessen worden getrokken die bijdragen aan het verhogen van de weerbaarheid in Nederland. **De leden van de VVD vragen daarnaast expliciet naar het functioneren van de nationale crisisorganisatie en of deze geëvalueerd gaat worden.** Voor een crisis in het digitale domein met aanzienlijke maatschappelijke gevolgen is het Nationaal Crisisplan Digitaal opgesteld, dit plan sluit aan op het Nationaal Handboek Crisisbesluitvorming. Het Nationaal Crisisplan Digitaal (NCP-Digitaal) is in februari door dit kabinet vastgesteld en met uw Kamer gedeeld[10]. Het plan is een leidraad om op hoofdlijnen snel inzicht en overzicht te creëren in de bestaande afspraken op nationaal niveau en de aansluiting met de betrokken publieke en private partners op regionaal/lokaal en internationaal niveau. Ik wil de lessen die voortkomen uit de Citrix evaluatie expliciet meenemen in de actualisering van het NCP-Digitaal die nog ter hand wordt genomen voor het einde van 2020. Deze evaluatie en de door het COT op verzoek opgestelde aanvullende reflectie op het NCP-Digitaal biedt aanvullende punten om mee te wegen in deze actualisering. **De leden van de GL-fractie en VVD-fractie vragen naar een evaluatie over het functioneren van het NCSC. De GL-fractie vraagt in aanvulling of ik bereid ben de rol van het NCSC bij digitale crisisbeheersing nog eens tegen het licht te houden.** Ik kan u daarover zeggen dat er bij de Citrix-evaluatie onder leiding van het COT een lessensessie heeft plaatsgevonden ten aanzien van het optreden van het NCSC binnen het Landelijk Dekkend Stelsel. De bevindingen daaruit zijn reeds verwerkt in de evaluatie door het COT die uw Kamer heeft ontvangen. De rol van het NCSC neem ik mee in het opstellen van het responskader voor incidenten met een digitale component. **De leden van de CDA-fractie vragen of er geen aanleiding is juist de start van het Citrix-incident, de melding en het assessment van dat incident aan een nadere evaluatie te onderwerpen, inclusief de vraag welke betekenis kan en moet worden toegekend aan de termijn van 90 dagen waarbinnen een leverancier de tijd krijgt om een lek te herstellen. In dat kader vragen de leden van de CDA-fractie of zij de rapportage van het COT juist hebben gelezen in die zin dat het COT naar de primaire waardering van het beveiligingsincident geen onderzoek heeft gedaan, maar deze als uitgangspunt heeft aangenomen.** Zoals ik eerder heb aangegeven was de scope van de evaluatie de werking van het gehele stelsel. De brief aan uw Kamer van 23 januari[11] kunt u raadplegen voor meer achtergrond over de keuzes die zijn gemaakt ten aanzien van de waardering van het beveiligingsincident. Ik hoop u daarmee voldoende inzicht te hebben verschaft in hoe de gegeven adviezen tot stand zijn gekomen. Ten aanzien van de termijn van 90 dagen kan ik u aangeven dat dit gaat om een gebruik binnen de industrie. Ik ga echter niet over de bedrijfsvoering van het Amerikaanse bedrijf Citrix, inclusief de van toepassing zijnde hersteltermijn van kwetsbaarheden in hun producten. Mijn focus ligt op het zo veel mogelijk

[9] Kamerstukken 26 643 en 30 821, nr.673
[10] Kamerstuk 30 821, nr. 102
[11] Kamerstuk 26 643, nr. 660

beperken van de impact van de betreffende kwetsbaarheden in Nederland.

De leden van de VVD-fractie vragen zich af voor wat betreft het toekomstige gebruik van het Citrix systeem van de rijksoverheid welke lessen zijn getrokken uit het Citrix-incident. Daarnaast vragen zij zich af hoe veilig de huidige manier is waarop de rijksoverheid gebruik maakt van het Citrix systeem. Voor het gebruik van alle software binnen de rijksoverheid zijn eisen en richtlijnen opgesteld door mijn collega van BZK. Deze gelden ook voor Citrix. Het is primair de verantwoordelijkheid van iedere organisatie binnen de rijksoverheid om deze regels na te leven en toe te passen in zijn systemen. CIO Rijk monitort dit. Als ontwikkelingen daar aanleiding toe geven kunnen deze eisen en regels worden aangepast.

De leden van de GL-fractie vragen of er een schatting is gemaakt van de financiële en andere kosten rondom de Citrix problematiek. Over een algehele schatting beschik ik niet.
De leden van de GL-fractie vragen ook hoeveel organisaties en werknemers zijn geraakt door het Citrix-incident. Het precieze aantal kan ik u niet geven omdat ik niet beschik over het volledige klantenbestand van Citrix in Nederland. **De leden van de GL-fractie stellen in dat kader de vraag in hoeverre bedrijven en de overheid verzekerd zijn tegen de gelopen schade naar aanleiding van de Citrix problematiek van januari 2020.** Er is mij niet bekend in hoeverre het vitale en niet-vitale bedrijfsleven verzekerd was voor de schade opgelopen door de kwetsbaarheden in Citrix-ADC en Citrix-Gateway. Dit is een overweging van bedrijven zelf. De overheid sluit in de regel voor dergelijke aangelegenheden geen verzekeringen af voor zichzelf en is dus niet verzekerd voor dit soort schade.

De leden van de GL-fractie vragen of ik iets kan zeggen over de verantwoordelijkheid voor de kwetsbaarheid in de betreffende Citrix producten. De producent van de software is in beginsel verantwoordelijk voor kwetsbaarheden in de software en het ontwikkelen van oplossingen voor deze kwetsbaarheden. Dat dit soort kwetsbaarheden ontstaan is niet uit te sluiten, het ontwikkelen van software is voor een groot deel mensenwerk en hierbij kunnen fouten worden gemaakt waardoor kwetsbaarheden ontstaan. In een gedigitaliseerde maatschappij kunnen dit soort kwetsbaarheden grote impact hebben. Het is daarom wel belangrijk dat aanbieders zo snel mogelijk een oplossing aanbieden voor de gevonden kwetsbaarheden. In het geval van Citrix heeft het NCSC over het uitkomen van een sluitende oplossing in contact gestaan met Citrix en heeft aangedrongen op het snel beschikbaar stellen van een sluitende oplossing. **De leden van de GL-fractie vragen naar de schaal die is gebruikt bij de inschaling van de kwetsbaarheid in Citrix ADC en Citrix Gatewayservers.** Kwetsbaarheden worden door het NCSC behandeld aan de hand van een inschalingsmatrix[12]. Het NCSC heeft de Citrix-kwetsbaarheid aanvankelijk ingeschaald op een middelgrote kans op misbruik met een hoge kans op schade bij misbruik, en heeft dit later bijgesteld naar de hoogste classificatie (hoog/hoog). Deze kwetsbaarheid werd middels de Common Vulnerability Scoring System (CVSS) door Citrix zelf qua ernst ingeschaald op een 9,8 op een schaal van 1 t/m 10. Deze CVSS-score is input voor de uiteindelijke inschaling van een kwetsbaarheid door het NCSC. **De leden van de GL-fractie vragen daaropvolgend waarom het dringende advies tot uitschakelen van de betreffende Citrix systemen drie dagen later kwam na inschaling van 9,8 op 17 januari**. Voor een uitgebreid overzicht van

[12] Zie https://www.ncsc.nl/documenten/publicaties/2019/juli/02/inschalingsmatrix

gebeurtenissen in deze periode verwijs ik uw kamer naar de brief van 23 januari[13]. Hierin wordt uitgebreid de aanloop beschreven richting het advies omtrent het uitschakelen van de betreffende Citrix systemen. Eveneens vragen dezelfde leden of de inschaling in die periode verder is opgelopen. Dat is niet het geval geweest.

De leden van de GL-fractie vragen mij wat ik van de signalen vond dat het voor veel organisaties onduidelijk was wie de regie voerde tijdens de Citrix-kwetsbaarheid. Wat mij betreft zijn dit signalen om serieus te nemen, de NCTV neemt deze dan ook mee in de actualisatie van het Nationaal Cisisplan Digitaal. Daarnaast heb ik in de kabinetsreactie op het WRR-rapport «Voorbereiden op digitale ontwrichting»[14] verschillende maatregelen aangekondigd die bijdragen aan het aanscherpen van de verschillende rollen en verantwoordelijkheden tijdens een digitaal incident. Zo werkt de NCTV samen met het NCSC aan een handreiking Landelijk Dekkend Stelsel (LDS) waarbinnen de verschillende rollen en mogelijkheden tijdens en voorafgaand aan een digitaal incident worden geschetst voor partijen die niet binnen de primaire doelgroepen van het NCSC (rijksoverheid of vitale aanbieders) vallen. Een ander voorbeeld is de uitwerking van het responskader bij digitale incidenten. Dit kader maakt inzichtelijker wat de rollen van de verschillende operationele partijen zijn tijdens een digitaal incident. **De leden van GroenLinks vragen mij wat de gevolgen zijn van meer nationale regie door de overheid voor wat betreft aansprakelijkheid**. Wat meer nationale regie voor de aansprakelijkheid betekent hangt af van de precieze invulling van deze regie en de omstandigheden. In het algemeen kunnen we stellen dat adviezen vanuit de rijksoverheid die oproepen tot bijvoorbeeld het weren van bepaalde producten consequenties kunnen hebben voor de desbetreffende producent, die hierdoor mogelijk juridische stappen zal overwegen. Daarom worden dit soort vergaande adviezen alleen gegeven als er sprake is van een aantoonbaar risico voor de nationale veiligheid. **De leden van de GL-fractie vragen in hoeverre er gedurende de periode van de Citrix problematiek contact is geweest met de cybersecurity-diensten van andere lidstaten en van de Europese Commissie om adviezen en maatregelen onderling af te stemmen?** Zoals ik al in mijn eerste brief hierover op 20 januari 2020 heb aangegeven staat het NCSC in voortdurend contact met internationale partners[15]. Ook gedurende de periode rondom de Citrix problematiek is meerdere malen contact en afstemming geweest met collega-organisaties in het buitenland. Het NCSC heeft t.o.v. andere partners een stevig advies gegeven. Het advies van mijn ministerie op 17 januari 2020 om waar mogelijk Citrix uit te schakelen was mede op basis van een beveiligingsadvies van de AIVD. Nederland is een land dat in sterke mate gedigitaliseerd is en daarnaast kent Nederland een groot aantal klanten van Citrix-producten. Daarmee kan de impact van een kwetsbaarheid in deze producten dan ook groot zijn, waardoor een stevig advies als passend is beoordeeld. Organisaties in andere landen maken hun eigen afwegingen op basis van hun nationale situatie en komen zodoende zelf tot een advies dat passend is voor het betreffende land.

De leden van de CDA-fractie vragen om – zo nodig vertrouwelijk – de Kamer te informeren waar de inlichtingeninformatie uit bestond, die werd gebruikt voor de inschatting dat de kwetsbaarheid daadwerkelijk zou worden misbruikt en waarschijnlijk zelfs al werd misbruikt. In het openbaar worden geen uitspraken

[13] Kamerstuk 26 643, nr. 660
[14] Kamerstukken 26 643 en 30 821, nr. 673
[15] Kamerstuk 26 643, nr. 658

gedaan over het kennisniveau en de werkwijzen van de inlichtingen- en veiligheidsdiensten. In voorkomende gevallen kan de Kamer via de geëigende kanalen worden geïnformeerd. **De leden van de CDA-fractie vragen welke maatregelen genomen worden om juist in de diagnose-fase van een (groot) cyberincident meer kennis en kunde in te bouwen en vragen of hierbij wordt meegenomen dat het NCSC niet zelf in staat is om diepgaander technisch onderzoek uit te voeren en hierbij afhankelijk is van andere partijen. Ten aanzien van dat laatste vragen zij welke andere partijen dit zijn**. Sinds het uitbrengen van de Nederlandse Cybersecurity Agenda (NSCA) in 2018 werkt het kabinet aan de daarin vervatte ambities en doelstellingen waaronder het op orde brengen van de slagkracht. Er wordt voortdurend gewerkt om deze slagkracht te vergroten en incidenten uit het verleden te evalueren om te bepalen wat nodig is in de toekomst. Een van de initiatieven voor het versterken van de kennispositie en daardoor de taakuitoefening van publieke partijen en het als gevolg daarvan meer en sneller bieden van het handelingsperspectief aan belanghebbende organisaties, is het in de kabinetsreactie op het WRR-rapport aangekondigde samenwerkingsplatform tussen het NCSC, AIVD, MIVD, OM en Politie. Juist door het zo veel als mogelijk bijeenbrengen van informatie en het verrichten van gezamenlijke analyses, kan in de diagnose-fase kennis en kunde bijeengebracht worden en meer handelingsperspectief worden gecreëerd. Daarnaast is het belangrijk om te benadrukken dat elk cyberincident anders is. Sommige incidenten komen voor in systemen die bijvoorbeeld specifiek zijn voor een bepaalde organisatie of sector en alleen daarbinnen – in de eigen organisatieomgeving en context – gebruikt worden. In zulke gevallen zal het NCSC waar mogelijk schakelen met organisaties in de doelgroep (Rijk, vitaal) of met een sectoraal computercrisisteam, om gebruik te maken van hun sectorspecifieke kennis en kunde van de in die sector gebruikte systemen. Tenslotte zijn organisaties in beginsel zelf verantwoordelijk voor het organiseren van hun digitale veiligheid en het nemen van passende maatregelen om cyberincidenten op juiste wijze af te handelen. De private cybersecuritysector heeft daarbij een belangrijke rol en voert op contractbasis vaak als eerste technisch onderzoek uit naar een cyberincident bij een organisatie.

3. WRR

De leden van de PVV-fractie vragen of ik vind dat cyber gerelateerde onderwerpen centraler opgepakt moeten worden door bijvoorbeeld een Cybercommissaris aan te stellen zoals voorgesteld in het Deltaplan Cybersecurity. In de ogen van de leden leidt het overlaten van cyber gerelateerde problemen aan vakminister tot een versnipperde aanpak. Digitale veiligheid moet geborgd zijn binnen elk domein en een centraal onderdeel worden van de reguliere beveiligingsstructuur. De verschillende betrokken departementen moeten samen, maar vanuit hun eigen rol en verantwoordelijkheid met deze opgave aan de slag. Als coördinerend bewindspersoon zie ik het als mijn taak om dit werk niet van hen over te nemen, maar mijn collega's aan te sporen of te adviseren. Een te gecentraliseerde aanpak van cyber gerelateerde onderwerpen leidt wat mij betreft tot een verlies van expertise en verantwoordelijkheid. Wel ben ik het met de bovengenoemde leden eens dat we moeten waken voor een te versnipperde aanpak. Afgelopen jaar heb ik geprobeerd om dit binnen de huidige kaders zoveel mogelijk samen te brengen. De lessen uit de evaluatie van de Citrix-problematiek later zien dat verdere stappen mogelijk nodig zijn. Daarom heb ik in de kabinetsreactie op het WRR-rapport «Voorbereiden op digitale ontwrichting» verschillende trajecten aangekondigd waarmee ik het huidige stelsel in kaart breng, eventuele tekortkomingen zal signaleren en

als sluitstuk de Wet beveiliging netwerk- en informatiesystemen (Wbni) wil wijzigen. Bij de Kamerbrief met de beleidsreactie op het CSNB2020 en de voortgangsrapportage NCSA informeer ik u over de tijdlijn en de gewenst opbrengst. **De leden van de PVV-fractie vragen mij ook wanneer het wetgevingstraject van de wijziging Wbni wordt gestart.** De start van het wetgevingstraject is afhankelijk van de hierboven genoemde verkenning en zal ik uw Kamer ook bij de CSBN/NCSA-brief nader over informeren.
De leden van de PVV-fractie en de SP-fractie vragen waarom ik geen afgebakende wettelijke bevoegdheid creëer voor digitale hulptroepen en ook geen onderzoek doe naar een aparte regeling voor overheidshandelen gericht op tegengaan van escalatie terwijl dit wel door de WRR wordt aanbevolen. Digitale incident-respons moet altijd onderdeel zijn van de reguliere incident-respons, omdat fysieke incidenten ook bijna altijd digitale elementen kennen en vice versa. Om dit bij elkaar te brengen is er ter specificering van het nationaal handboek crisisbesluitvorming het Nationaal Crisisplan Digitaal (NCP-Digitaal) ontwikkeld. Daarnaast zal er een nationaal responskader worden uitgewerkt waarin de handelwijze van de verschillende operationele partijen in geval van een digitaal incident wordt uitgewerkt. Ook laat ik een brede verkenning uitvoeren naar de bevoegdheden die zijn vastgelegd in (sectorale)wetgeving om bijvoorbeeld in te grijpen bij digitale incidenten om te bezien of hier aanvullingen nodig zijn. **Dezelfde leden willen daarnaast ook weten hoe de digitale hulptroepen er uitzien en of dit bijvoorbeeld wordt belegd bij het Nationaal Cybersecurity Centrum (NCSC) en of het NCSC hiervoor wel voldoende capaciteit heeft.** Veel organisaties hebben hun eigen digitale response capaciteit ingericht, het adequaat kunnen reageren tijdens een digitaal incident vergt een uitgebreide en actuele kennis van de in de desbetreffende organisatie in gebruik zijnde netwerk- en informatiesystemen. Organisaties zijn in beginsel namelijk zelf verantwoordelijk voor het borgen van snel herstel na een incident. Daarnaast heeft het NCSC de taak om partijen binnen de doelgroep rijksoverheid en vitaal bijstand te verlenen. Het NCSC verstrekt in dit verband deze partijen dreigingsinformatie en biedt handelingsperspectief aan de hand waarvan de beveiligingsexperts van die partijen kunnen handelen. Daarnaast coördineert het NCSC het Nationaal Respons Netwerk (NRN) waarbinnen verschillende computercrisisteams samenwerken om bij grootschalige incidenten elkaar van bijstand te kunnen voorzien. Hierdoor kan het NCSC in voorkomende gevallen een verzoek doen tot meer capaciteit als dit nodig is.

De leden van de PVV-fractie willen weten hoe het kabinet – met onverminderde inzet en investeringen- ons land digitaal veilig gaat houden en zich voorbereidt op digitale incidenten. Cybersecurity is een prioriteit van dit kabinet en er zijn al veel belangrijke maatregelen in gang gezet bij de overheid, (vitale) bedrijven en andere organisaties. Deze maatregelen richten zich op preventie, maar ook op onze respons op digitale incidenten. Ook de komende periode zal om onze digitale weerbaarheid te borgen over de hele breedte geïnvesteerd moeten worden om de ontwikkelingen bij te kunnen houden. Voor een overzicht van concrete stappen die zullen worden gezet om Nederland digitaal veilig te houden verwijs ik u graag naar de tabel «Versterking Cybersecuritystelsel: Respons en Weerbaarheid» in de kabinetsreactie op het WRR rapport «Voorbereiden op digitale ontwrichting»[16]. De Cyber Security Raad zal daarnaast eind 2020 een advies geven over waarin volgens hen de komende jaren geïnvesteerd moet worden om Nederland digitaal veilig te houden. **De leden van de D66-fractie vragen**

[16] Kamerstukken 26 643 en 30 821, nr. 673

wanneer ik kan aangeven dat Nederland wél voldoende is voorbereid op digitale ontwrichting. De overheid neemt een tal van maatregelen om de digitale weerbaarheid te verhogen en ons zo goed mogelijk voor te bereiden op digitale incidenten. Dit zijn preventieve maatregelen bijvoorbeeld via regelgeving (beveiligingseisen) en voorlichting, maar ook detectie- en responsemaatregelen en – in geval van strafbare feiten bij cybercrime -opsporing en vervolging. Dit blijft echter een enorme uitdaging die wordt vergroot door de snelheid waarmee digitale technologie en het gebruik daarvan zich ontwikkelt. **De leden van D66 vragen vervolgens welke indicatoren ik gebruik om vast te stellen of we voldoende voorbereid zijn en of ik over voldoende middelen en bevoegdheden beschik.** Digitale weerbaarheid van Nederland is een breed concept waar helaas geen alomvattend meetinstrument voor is. Het beeld van onze weerbaarheid baseren we op verschillende onderzoeken en instrumenten. Sectorale toezichthouders hebben zicht op de weerbaarheid van vitale aanbieders en werken aan een inspectiebeeld cybersecurity waarmee inzicht wordt verkregen in de weerbaarheid van de vitale infrastructuur. Ook rapporten van bijvoorbeeld de Algemene Rekenkamer bieden inzicht. Dit soort rapportages laten steeds zien dat er stappen zijn genomen maar ook dat er nog enorm veel moet gebeuren om alle ontwikkelingen bij te houden en dat we ook de komende jaren over de hele linie moeten investeren in onze digitale weerbaarheid.

De leden van de SP-fractie vragen zich af of de overheid niet achter de feiten heeft aangelopen gezien de uitspraken van de WRR over het ontbreken van een uitgebreide crisisorganisatie voor digitale incidenten en waarom de regering dit WRR-rapport nodig heeft gehad om in actie te komen. Ik onderstreep de conclusie dat een goed functionerende samenleving weerbaar is in het fysieke domein én in het digitale domein. Daarom is een van de NCSA prioriteiten ook slagkracht op orde brengen, en is daar ook door dit kabinet in geïnvesteerd. De afgelopen jaren hebben we stappen gezet om onze digitale weerbaarheid te verhogen en ons voor te bereiden op een crisis met digitale elementen. Ik vind daarom niet dat we ons pas veel te laat bewust werden van de problematiek. Het meest concrete voorbeeld hiervan is de ontwikkeling van het Nationaal Crisis Plan Digitaal (NCP-digitaal) dat in februari naar uw Kamer is verzonden. De eerste versie van dit crisisplan is in 2011 ontwikkeld. Het WRR rapport onderstreept wat mij betreft nogmaals het belang van deze en nieuwe maatregelen en is daarmee een welkome waarschuwing. **De leden van de SP-fractie vragen mij hoe ik het kan verklaren dat alle maatregelen die tot nu toe door de regering zijn genomen gericht zijn op preventie terwijl de WRR erop wijst dat cyberaanvallen niet zijn te voorkomen maar vooral de vraag is wat ertegen te doen valt.** We kunnen cyber aanvallen nooit helemaal voorkomen, maar we kunnen met behulp van preventieve maatregelen het aantal en de impact wel sterk beperken. Bovendien helpen maatregelen die zijn gericht op preventie en paraatheid ook vaak bij snel herstel na een cyberaanval. Bijvoorbeeld door vooraf een incidentresponsplan op te stellen en deze te oefenen zodat wanneer een incident zich voordoet men adequaat kan reageren en de (vitale) dienstverlening snel hersteld kan worden. Daarnaast neemt dit kabinet wel degelijk maatregelen die ons in staat stellen snel en adequaat te reageren op digitale incidenten. Hierbij valt te denken aan de oprichting van het Nationaal Respons Netwerk en de ontwikkeling van het NCP-Digitaal.

De leden van de SP-fractie vragen waarom de verantwoordelijkheid voor de beveiliging van vitale digitale infrastructuren bij individuele aanbieders ligt in plaats van bij de overheid. De vitale

aanbieders zijn in beginsel zelf verantwoordelijk voor de continuïteit van de essentiële dienst en dienen maatregelen te nemen die deze continuïteit waarborgt; zij hebben dus een zorgplicht. De overheid werkt deze zorgplicht momenteel nader uit in een wijziging van het Besluit Beveiliging Netwerk- en Informatiesystemen (Bbni). Hoe vitale aanbieders vervolgens in concreto aan de bij en krachtens de Wet beveiliging netwerk en informatiesystemen (Wbni) gestelde plicht tot het nemen van beveiligingsmaatregelen voldoen bepalen zij in beginsel zelf. Welke maatregelen passend zijn varieert per sector of organisatie en hier is maatwerk voor nodig. Dit vergt diepgaande kennis van de organisatie en de gebruikte netwerk en informatiesystemen. Dit betekent niet dat het beveiligen van de vitale digitale infrastructuren vrijblijvend is, zij moeten aan de zorgplicht voldoen. De overheid houdt hier toezicht op.
De leden van de GroenLinks-fractie willen weten of het klopt dat ik de aanbeveling uit het WRR rapport om een jaarlijks Cyberafhankelijkheidsbeeld op te stellen niet overneem omdat vitale aanbieders daar zelf verantwoordelijk voor zijn. Daarnaast willen de leden weten of ik de analyse van de leden deel dat de optelsom van individuele afhankelijkheden onvoldoende bekend is waardoor zo'n cyberafhankelijkheidsbeeld van groot belang is aangezien digitale risico's het niveau van individuele aanbieders overstijgen gezien de sterke netwerkeffecten. Ik onderschrijf het belang van inzicht in afhankelijkheden. De onderlinge afhankelijkheid neemt toe en dit maakt ons kwetsbaar. De WRR doet de aanbeveling om een cyberafhankelijkheidsbeeld op te stellen en maakt hierbij de vergelijking met het Cybersecuritybeeld Nederland. Het kabinet is echter niet overtuigd dat een jaarlijks beeld gaat helpen bij het verkrijgen van de benodigde inzichten. Een jaarlijks beeld is statisch terwijl dit soort afhankelijkheden zich snel ontwikkelen waardoor zon beeld niet bijdraagt aan het uiteindelijke doel: het verhogen van onze digitale weerbaarheid. Wat hier wel aan bijdraagt is organisaties die zelf bewust zijn van hun afhankelijkheden en wat voor kwetsbaarheden deze afhankelijkheden met zich meebrengen. Sectorale toezichthouders kunnen vervolgens beoordelen of aanbieders van essentiële diensten dit voldoende in beeld hebben. De leden van GroenLinks maken hierbij een valide punt dat juist ook de optelsom van individuele afhankelijkheden tot inzicht leidt over kwetsbaarheden. In de versterkte aanpak vitale infrastructuur, waarover ik uw Kamer de tweede helft van 2020 zal informeren, zal daarom ook aandacht zijn voor wederzijdse afhankelijkheden. **De leden van de GroenLinks-fractie en de SP-fractie vragen zich af hoe ik er voor ga zorgen dat organisaties daadwerkelijk aan terugvalopties denken bij het opstellen van hun risico analyse. Daarnaast willen de leden weten hoe ik tegen de mogelijkheid aankijk om terugvalopties te verplichten.** Bij het organiseren van terugvalopties spelen verschillende belangen zoals veiligheid op locatie, continuïteit en mogelijke investeringen waarover een afweging gemaakt dient te worden. In principe kunnen aanbieders van essentiële diensten deze afweging het best zelf maken, wat niet betekent dat het vrijblijvend is. Krachtens de Wbni zijn aanbieders van essentiële diensten (AED) verplicht om passende en evenredige technische en organisatorische beveiligingsmaatregelen met betrekking tot hun netwerk- en informatiesystemen te nemen, onder andere om de gevolgen van incidenten zoveel mogelijk te beperken. Die maatregelen kunnen bijvoorbeeld ook het organiseren van terugvalopties betreffen. De toezichthouder ziet er op toe dat AED's genoemde maatregelen treffen en zal aanbieders ook kritisch bevragen wanneer zij niet kunnen aantonen dat zij een juiste risico analyse hebben gedaan of mitigerende maatregelen hebben getroffen ter verkleining van de risico's tot een aanvaardbaar niveau. Momenteel is ter nadere invulling van de plicht tot het treffen van voldoende beveiligingsmaatregelen in de Wbni een wijziging van het daarop gebaseerde Bbni in voorbereiding. Ook

zal het hierdoor mogelijk zijn de zorgplicht voor één of meerdere sectoren nader uit te werken in een ministeriële regeling. Ook kan een nadere invulling hiervan door de sectorale toezichthouders plaatsvinden. **De leden van de D66-fractie willen weten of ik het met hen eens ben dat het mandaat van het NCSC op het gebied van informatie-deling en de mate waarin het doorvoeren van cruciale updates afgedwongen kan worden door het NCSC beiden versterkt moeten worden om toekomstige situaties beter het hoofd te kunnen bieden.** Ik ben van mening dat beschikbare updates in principe altijd zo snel mogelijk geïnstalleerd moeten worden. Het kan echter zo zijn dat het snel doorvoeren van een update impact kan hebben op de continuïteit van de (vitale) dienstverlening. Als een update bijvoorbeeld als gevolg heeft dat een deel van Nederland geen stroom meer heeft dan weegt dat soms niet op tegen de risico's van het niet uitvoeren van de update. Daarom werkt dit kabinet samen met de vitale aanbieders en de sectorale toezichthouders aan een «pas toe of leg uit» methodiek. Bij ernstige beveiligingsadviezen van het NCSC moeten vitale aanbieders aan de sectorale toezichthouder uitleggen wat de overwegingen zijn voor het niet uitvoeren van belangrijke updates. Ik ben het daarnaast met de leden van D66 eens dat informatie-uitwisseling met het NCSC versterkt moet worden. Ook binnen de huidige wettelijke kaders kan echter al veel bereikt worden. Zo werk ik aan het verbeteren van de informatiedeling tussen NCSC en toezichthouders en het verbreden van het Landelijk Dekkend Stelsel door het aanwijzen van meer sectorale cybersecurity organisaties waarmee ook bepaalde vertrouwelijke informatie gedeeld kan worden. Tegelijkertijd inventariseer ik de wettelijke bevoegdheden om in te grijpen bij incidenten met een digitale component en beoordeel ik of aanvullingen nodig zijn.

De leden van de GroenLinks-fractie informeren naar de deadline en reikwijdte van de verkenning naar de wettelijke bevoegdheden bij het ingrijpen tijdens een digitale crisis. De leden vragen hierbij naar de bevoegdheden bij digitale incidenten waar de nationale veiligheid niet in het geding is en naar de bevoegdheden met betrekking tot zowel vitale als niet-vitale organisaties. Ik verwacht deze verkenning begin 2021 af te ronden. De verkenning focust zich op bevoegdheden die het kabinet heeft om in te grijpen bij een digitale crisis. Het doel is om het beschikbare instrumentarium voor zowel vitale als niet-vitale organisaties inzichtelijk te krijgen. Over de precieze invulling van deze verkenning zal ik uw Kamer zoals hierboven ook aangegeven in de Kamerbrief CSBN2020/Voortgang NCSA informeren. **De leden van de VVD-fractie vragen zich af hoe het in de kabinetsreactie genoemde samenwerkingsplatform zich zal verhouden tot het aangekondigde nationale responskader.** Zoals in de kabinetsreactie benoemd, heeft het samenwerkingsplatform tot doel om informatie over cyberdreigingen en -incidenten door verschillende publieke partijen (AIVD, NCSC, etc.) bijeen te brengen en gezamenlijke analyses te verrichten en hierdoor meer en sneller handelingsperspectief aan belanghebbende organisaties te kunnen bieden. Het nationale respons-kader ziet echter op afspraken tussen een breder aantal partijen over incidentrespons in geval van een incident met digitale componenten. Beiden zullen complementair zijn aan elkaar.

De leden van de VVD-fractie vragen of ik een overzicht kan geven van vitale aanbieders met zowel een meld- als zorgplicht en van vitale aanbieders met alleen een meldplicht. Voor een overzicht van de (categorieën van) vitale aanbieders, die hetzij als aanbieder van essentiële diensten (AED), hetzij als andere aangewezen vitale aanbieders (AAVA) zijn aangewezen verwijs ik u graag naar het overzicht hiervan in

het Bbni. Voor digitale dienstverleners en AED's[17] geldt op grond van de Wbni zowel de zorgplicht als een dubbele meldplicht.[18] Voor AED's betekent dit dat voor hen een meldplicht geldt bij zowel het NCSC als bij de respectievelijke sectorale toezichthouder. Voor digitale dienstverleners betekent dit dat voor hen een meldplicht geldt bij zowel het CSIRT-DSP als bij het Agentschap Telecom. Daarnaast geldt voor AED's ook de zogenaamde «zorgplicht».[19] Voor AAVA's[20] geldt op grond van de Wbni een enkele meldplicht bij het Nationaal Cyber Security Centrum (NCSC). Sommige AAVA's, zoals de telecomaanbieders[21] hebben krachtens sectorale wetgeving al een meldplicht bij een sectorale toezichthouder en een zorgplicht, waardoor deze verplichtingen niet voor hen in de Wbni zijn opgenomen. **De leden van de VVD-fractie vragen in hoeverre grote, niet-vitale bedrijven kunnen worden voorzien van voldoende specifieke informatie over digitale dreigingen door bijvoorbeeld een sectorale toezichthouder.** Grote niet vitale bedrijven vallen over het algemeen niet onder een sectorale toezichthouder. Zij kunnen op diverse andere manieren worden voorzien van informatie over digitale dreigingen. Zo maken zij voor de continuïteit en beveiliging van hun digitale diensten vaak gebruik van commerciële aanbieders die hen van relevante informatie voorzien. Ook kan het NCSC voor niet-vitale bedrijven relevante aanvullende informatie over dreigingen en incidenten, die in het kader van de reguliere taakuitoefening is verkregen, delen met aangewezen sectorale cybersecurity organisaties die tot taak hebben om bepaalde niet-vitale bedrijven daarover te informeren zodat deze organisaties op hun beurt dergelijke informatie onder hun doelgroepen verspreiden. Hierbij is het wel van belang dat organisaties zich verenigen in een sectorale cybersecurity organisatie waarmee die informatie gedeeld kan worden. Daarnaast kunnen niet-vitale bedrijven terecht bij het Digital Trust Center (DTC) voor informatie en advies in het algemeen. Op dit moment wordt er door het Ministerie van EZK gewerkt aan het voldoen aan de voorwaarde voor de aanwijzing van het DTC krachtens de Wbni als OKTT, zodat ook via het DTC specifieke informatie over dreigingen en incidenten kan worden gedeeld. **De leden van de VVD-fractie vragen aansluitend of ik een overzicht kan geven welke sectoren wel en welke geen sectorale toezichthouder kennen.** Wanneer in de context van cybersecurity gesproken wordt over een sectorale toezichthouder worden in het bijzonder toezichthouders bedoelt die zijn aangewezen onder de Wet beveiliging netwerk- en informatiesystemen (Wbni). Deze wet voorziet uitsluitend in handhaving ten aanzien van de verplichtingen voor aanbieders van essentiële diensten (AED's), een subcategorie van vitale aanbieders, en digitale dienstverleners. Voor digitale dienstver-

---

[17] Aangewezen vitale aanbieders in de sectoren: energie, digitale infrastructuur, bankwezen, infrastructuur voor de financiële markt, vervoer, levering en distributie van drinkwater en digitale infrastructuur.

[18] Hierbij gaat het om een meldplicht bij de toezichthouder en het NCSC voor incidenten met aanzienlijke gevolgen voor de continuïteit van de door hen verleende diensten, en bij de meldplicht bij het NCSC, ook om inbreuken op de beveiliging van hun netwerk- en informatiesystemen die aanzienlijke gevolgen kunnen hebben («bijna-ongelukken») voor de continuïteit van de verleende dienst.

[19] Hierbij gaat het om de verplichting om passende technische en organisatorische maatregelen te nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen, de plicht om passende maatregelen te treffen om incidenten te voorkomen die de beveiliging aantasten van de voor de verlening van de dienst gebruikte netwerk- en informatiesystemen én de plicht om de gevolgen van dergelijke incidenten zo veel mogelijk te beperken.

[20] Aangewezen vitale aanbieders in de sectoren: nucleair, keren en beheren, financieel en elektronische communicatienetwerken en -diensten/ICT.

[21] De meldplicht en zorgplicht in de Telecommunicatiewet (Tw) geldt voor alle aanbieders van openbare elektronische communicatienetwerken en/of diensten; de Tw maakt geen onderscheid tussen vitaal en niet-vitaal.

leners is het Agentschap Telecom de sectorale toezichthouder. Voor AED's geldt het volgende:

AED-sector	Toezichthouder dienst
Energie	Agentschap Telecom
Digitale infrastructuur	Agentschap Telecom
Bankwezen	De Nederlandsche Bank N.V.
Infrastructuur voor de financiële markt	De Nederlandsche Bank N.V.
Vervoer	Inspectie Leefomgeving en Transport
Levering en distributie van drinkwater	Inspectie Leefomgeving en Transport
Gezondheidszorg[1]	Inspectie Gezondheidszorg en Jeugd

[1] Binnen deze sector is geen AED aangewezen

De leden van de D66-fractie vragen of ik nader in kan gaan op de mogelijkheid van het verbreden van het mandaat van het NCSC om relevante informatie ook te kunnen en mogen delen met partijen CERTS van niet-vitale sectoren, inclusief CERTS die tot taak hebben om leveranciers van essentiële ICT-diensten te ondersteunen, en hen te ondersteunen en zorg te dragen voor een actieve benadering van die partijen met kwetsbare systemen, die niet door een CERT vertegenwoordigd worden. De leden vragen of het kabinet bereid is om het mandaat van het NCSC hiertoe te verbreden, en de knelpunten die dit in de weg staan weg te nemen, en zo ja, op welke manier. Nederland kent een grote groep bedrijven die niet tot een vitale sector behoren: ongeveer 1,8 miljoen bedrijven. Die groep is niet alleen groot, maar ook erg divers als het gaat om hoe zij hun digitale processen hebben ingericht, hoe afhankelijk zij ervan zijn en wat hun volwassenheidsniveau is als het gaat om digitale veiligheid. Het DTC is een one stop cybersecurity shop voor het niet-vitale bedrijfsleven. Daarnaast fungeert het NCSC als aanspreekpunt voor andere aangewezen (sectorale) computercrisisteams en heeft het op grond van de Wbni de mogelijkheid om met deze sectorale computercrisisteams eventueel ook bepaalde vertrouwelijke dreigingsinformatie te delen. Naast het NCSC is ook het computer security incident response team voor digitale dienstverleners (CSIRT-DSP's) op grond van de Wbni als CSIRT aangewezen; het NCSC en het CSIRT voor digitale diensten werken zo veel mogelijk samen. Het CSIRT-DSP's kan eventueel ook andere computercrisisteams van informatie voorzien. Voor een optimale verspreiding van relevante informatie en de nodige schaalvergroting op dit gebied is het belangrijk dat sectoren zich in toenemende mate organiseren in samenwerkingsverbanden. Dit is de eigen verantwoordelijkheid van private en publieke organisaties. Het kabinet monitort de ontwikkeling van dit landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden voortdurend en kijkt waar verbeteringen nodig zijn. In de kabinetsreactie op het WRR-rapport «Voorbereiden op digitale ontwrichting» heb ik hiertoe verschillende trajecten aangekondigd. **De leden van de VVD-fractie vragen of ik kan aangeven in hoeverre vitale aanbieders worden geïnformeerd over «high end risks» door het NCSC.** Vitale aanbieders zijn een primaire doelgroep van het NCSC. Informatie over dreigingen en kwetsbaarheden wordt dan ook rechtstreeks aan vitale aanbieders verstrekt. Vitale aanbieders worden bijvoorbeeld over ernstige kwetsbaarheden die worden ingeschaald met een hoge kans op misbruik en een hoge (vervolg)schade actief geïnformeerd met informatie over welke mitigerende maatregelen getroffen kunnen worden. Bij de adviezen worden waar nodig en mogelijk ook de inzichten en informatie van nationale (veiligheids)partners en internationale CSIRT-collega's betrokken.

De leden van de PVV-fractie vragen wanneer de eerstvolgende actualisatie van het Nationaal Crisisplan Digitaal (NCP-Digitaal) is voorzien. De eerstvolgende actualisatie van het NCP-Digitaal wordt ter hand genomen voor het einde van 2020. **De leden van de VVD-fractie en GL-fractie vragen of de cyberoefening ISIDOOR wederom is uitgesteld tot 2021**. Hierover is uw Kamer per brief van 9 april[22] geïnformeerd. Ik kan u bevestigen dat ISIDOOR wordt uitgesteld tot een nader te bepalen moment in 2021. Voor de onderbouwing over dit besluit verwijs ik u door naar de eerdergenoemde brief van 9 april. **De leden van de VVD-fractie vragen hoe de cyberoefening ISIDOOR zich verhoudt tot de aangenomen motie van het lid Weverling dat vraagt om een structureel digitaal oefen- en stresstestprogramma.** Ik kan u daarover melden dat de oefening ISIDOOR integraal onderdeel uitmaakt van het genoemde programma. Deze oefening speelt een essentiële rol vanwege het belang van de oefening en de omvang van het aantal relevante deelnemers. **De leden van de GL-fractie en VVD-fractie stellen vervolgens vragen over de verschillende elementen en de verdere invulling van het oefenprogramma, naar aanleiding van de aangenomen motie van het lid Weverling.** Er wordt hard gewerkt aan de uitwerking van dit programma, waarbij ik alvast een korte toelichting zal geven op de drie sporen waarop wordt ingezet door dit kabinet. Over de voortgang hierop en de verdere uitwerking hiervan zal de Tweede Kamer jaarlijks worden geïnformeerd met de voortgangsbrief NCSA die ik nog voor het Zomerreces naar uw Kamer zal versturen. Het eerste spoor bestaat uit het door dit kabinet organiseren van grootschalige oefeningen in het kader van het Nationaal Crisisplan Digitaal. Het tweede spoor is de deelname van de overheid aan bestaande cyberoefeningen in verschillende sectoren. De aansluiting hierop is van belang om goed voorbereid te zijn en om leerpunten te signaleren in de samenwerking. Het derde spoor is het ontwikkelen van initiatieven op oefeningen in publiek privaat verband om oefeningen in verschillende sectoren verder te stimuleren. Zoals toegezegd informeer ik uw Kamer over de voortgang van het oefenprogramma bij de NCSA-voortgangsbrief die ik nog voor het Zomerreces naar uw Kamer zal versturen.

De leden van de CDA-fractie stellen verschillende vragen over vitale aanbieders. Allereerst of ik bereid ben om een vertrouwenspersoon binnen de vitale sectoren aan te stellen, zodat de NCTV/het NCSC specifieke informatie over externe dreigingen – zoals statelijke actoren – kan delen en de sector zich gerichter kan beschermen. Ik vind dat zeker een interessante suggestie. Dit punt zal ik nader verkennen als onderdeel van de reeds aangekondigde versterkte aanpak voor de bescherming van de vitale infrastructuur. **Daarnaast vragen ze of ik in overleg kan treden met de vitale sector en hen kan betrekken bij de versterkte aanpak vitaal zoals aangekondigd in de Nationale Veiligheid Strategie.** Dit ben ik zeker van plan, kenmerk van de bescherming van de vitale infrastructuur is nadrukkelijk een samenwerking met alle relevante partijen. Vanzelfsprekend worden dus ook de vitale aanbieders betrokken bij de versterkte aanpak. **De leden van de GroenLinks-fractie vragen of het huidige onderscheid tussen vitale en niet-vitale aanbieders gehandhaafd moet blijven gezien dat de WRR benadrukt dat ook het functioneren van niet-vitale toeleveranciers van grote invloed kan zijn op de continuïteit van vitale processen.** Ik besprak al eerder met u dat toeleveranciers heel belangrijk zijn voor het functioneren van de vitale processen. Dit is dan ook een belangrijk onderdeel van de versterkte aanpak vitale infrastructuur. **Deze leden vragen vervolgens of ik kan**

[22] Kamerstukken 35 300 VI en 25 295, nr. 116

aangeven wat dit betekent voor de rolverdeling tussen het NCSC en het DTC. Het NCSC en het DTC zijn complementair waarbij de rolverdeling tussen het NCSC en het DTC wordt bepaald aan de hand van verschillende doelgroepen. Het NCSC heeft primair tot taak organisaties binnen de rijksoverheid en vitale aanbieders van bijstand bij dreigingen en incidenten te voorzien. Daarnaast fungeert het, als centraal informatieknooppunt en expertisecentrum voor cybersecurity in Nederland, ook als aanspreekpunt binnen het LDS voor de andere sectorale computercrisisteams. Het DTC voorziet het niet-vitale bedrijfsleven van informatie en advies rondom dreigingen en kwetsbaarheden. Het NCSC en het DTC werken bij de uitoefening van hun onderscheidenlijke taken zo veel mogelijk samen. Partijen die in het kader van de versterkte aanpak vitale infrastructuur vitaal worden verklaard zullen daarmee onder de dienstverlening van het NCSC vallen. Toeleveranciers die niet vitaal zijn maar mogelijk wel diensten leveren ten behoeve van vitale processen vallen in beginsel binnen het domein van het DTC. Daarnaast is het streven om met de wijziging van het Besluit beveiliging netwerk- en informatie systemen als door aanbieders van essentiële diensten te nemen maatregel vast te leggen dat zij hun positie in de keten meenemen in de verplichte risico analyse. Dat betekent dat zij geen onveilige producten of diensten kunnen gebruiken ter ondersteuning van hun essentiële processen, omdat dit te grote risico's voor de veiligheid van de essentiële dienst zouden kunnen impliceren die niet kunnen worden gemitigeerd. Op de naleving hiervan door AED's vindt ook toezicht plaats. Voor sommige digitale dienstverleners (bijvoorbeeld verleners van cloudcomputerdiensten), die ook toeleveranciers van AED's kunnen zijn, gelden krachtens de Wbni, in samenhang met een Europese uitvoeringsverordening[23] ook wettelijke verplichtingen tot het treffen van beveiligingsmaatregelen. Hierop vindt ook toezicht plaats. Daarnaast vallen zij qua dienstverlening onder het CSIRT voor digitale diensten (CSIRT-DSP's).

De leden van de GroenLinks-fractie vragen of ik de WRR analyse deel dat veel processen die de publieke taak raken zijn uitbesteed aan private partijen, veelal gevestigd in het buitenland, waardoor er een afhankelijkheid wordt gecreëerd van partijen waarover de overheid maar in beperkte mate invloed kan uitoefenen, ook in deze crisistijd. De leden vragen wat deze afhankelijkheid betekent voor onze capaciteit om risico's in het digitale domein te beheersen. Tot slot vragen de leden of ik de mening deel dat de continuïteit van de samenleving hierdoor sterk afhankelijk is geworden van het doen en laten van private partijen en of deze afhankelijkheid niet te groot is. Nederland is als klein land met een open economie in grote mate afhankelijk van andere landen of partijen gevestigd in het buitenland. We zien dat in crisistijd deze afhankelijkheden sterker onder druk komen te staan. Ook in de Kamerbrief Tegengaan Statelijke dreigingen wordt dit benoemd[24]. Belangrijk hierbij is om zicht te hebben op mogelijke risico's zodat deze kunnen worden gemitigeerd, dit geldt uiteraard ook voor risico's in het digitale domein. Hier wordt door het kabinet op ingezet via verschillende instrumenten op o.a. het gebied van inkoop en aanbesteding, investeringen en overnames[25] en het beschermen van kennis en technologie. De leden vragen specifiek naar aanbestedingen, het kabinet heeft hiervoor het nationaal veiligheidsbeleid bij inkoop en aanbesteding geïmplementeerd. Overheidspartijen zijn er volgens dit beleid aan gehouden om bij de inkoop en aanbesteding van producten en diensten, waaronder ICT producten, een risicoanalyse te

[23] Uitvoeringsverordening (EU) 2018/151 van 30 januari 2018
[24] Kamerbrief tegengaan statelijke dreigingen 18 april 2019, Kamerstuk 30 821, nr. 72
[25] Zie ook de Kamerbrief Investeringstoets op risico's voor de nationale veiligheid Kamerstuk 30 821, nr. 97

maken en waar nodig maatregelen te nemen om ongewenste strategische afhankelijkheden, het risico op het in verkeerde handen vallen van gevoelige informatie of mogelijke verstoringen van de dienstverlening, te voorkomen of de eventuele impact daarvan te beperken. Afhankelijk van het type product of dienst kunnen de eisen die de overheid bij inkoop en aanbesteding stelt bepalend zijn voor de keuze van leverancier en additionele technische of organisatorische eisen worden gesteld. Het instrumentarium dat ter ondersteuning van dit beleid is ontwikkeld is ook ter beschikking gesteld aan vitale aanbieders. Ten slotte, het aanschaffen van ICT producten van buitenlandse, vaak niet Europese, ICT bedrijven is vaak moeilijk te vermijden. Niet Europese partijen domineren vaak de markt. Belangrijk is dat we hierbij voorkomen dat er onwenselijke strategische afhankelijkheden ontstaan met mogelijke risico's voor onze nationale veiligheid. Om deze reden verwelkomt het Kabinet de ambitieuze en integrale digitaliseringsagenda van de Europese Commissie. Nederland hecht grote waarde aan Europese samenwerking op digitalisering om gezamenlijk bij te dragen aan het versterken van Europees digitaal leiderschap waarbij waarden en regels van de Europese democratische en duurzame maatschappij geborgd blijven. Daar waar de publieke belangen in het geding komen door ongewenste afhankelijkheden op technologie uit derde landen zal de EU moeten kiezen voor het verminderen van deze strategische afhankelijkheden. Voor Nederland is daarbij de balans tussen een open economie en het beschermen van eigen economische en maatschappelijke waarden van belang. **De leden van de SP-fractie vragen mij of het niet beter zou zijn als de Nederlandse overheid zelf meer regie houdt over belangrijke digitale infrastructuren, bijvoorbeeld door de ontwikkeling van nieuwe software of digitale diensten binnen de Nederlandse grenzen te houden, zodat de Nederlandse toezichthouders kunnen toezien of de Nederlandse (digitale) samenleving wel voldoende wordt beschermd in geval van crisis**. Veel producten en diensten rond digitale infrastructuren en -diensten zijn samengesteld uit onderdelen die uit meerdere landen komen. Nederland kan zo als klein land profiteren van het kunnen afnemen en leveren van producten en diensten met goede kwaliteit en prijs. Daar waar de publieke belangen (zoals veiligheid, bescherming van persoonsgegevens en privacy, (keuze)vrijheid maar ook verdienvermogen) in het geding komen door ongewenste afhankelijkheden van technologie uit derde landen, zal Nederland moeten kiezen voor het verminderen van deze strategische afhankelijkheden. Zoals gezegd is de balans tussen een open economie en het beschermen van eigen economische en maatschappelijke waarden van belang. Het kabinet is van mening dat het verminderen van ongewenste afhankelijkheden van derde landen en eventueel stimuleren van nieuwe software of digitale diensten het best in Europees verband kan plaatsvinden. Het kosteneffectief ontwikkelen van kwalitatief hoogwaardige productensoftware van eenzelfde kwalitatief niveau als dat van sommige grote buitenlandse aanbieders, zowel met het oog op functioneren als digitale veiligheid, vraagt om doorlopende grote investeringen. Daarnaast is er Europese regelgeving om digitale infrastructuren te beschermen. Tenslotte is er ter uitvoering van Europese regelgeving nationale wetgeving om digitale infrastructuren te beschermen, op de naleving waarvan toezichthouders toezien (onder andere de Telecommunicatiewet en de Wet beveiliging netwerk- en informatiesystemen).

De leden van het CDA vragen mij uit te leggen welke rol het DTC (Digitale Trust Center) vervult als het gaat om cybersecurity? Het DTC is de one-stop cybersecurity shop voor het niet-vitale bedrijfsleven in Nederland en heeft tot doel deze bedrijven weerbaar(der) te maken tegen cyberdreigingen. Het DTC wil informatie en handelingsperspectieven op het gebied van cybersecurity ontsluiten aan het niet-vitale bedrijfsleven

op een niveau dat aansluit bij de behoefte van deze groep. Het DTC zal ook via eigen kanalen en via aangesloten samenwerkingsverbanden en individuele bedrijven informatie verzamelen die relevant is voor hun doelgroep. De focus in de eerste fase van het bestaan van DTC (2018–2020) is dat bedrijven in ieder geval een basisniveau van digitale veiligheid bereiken. In het verlengde van de conclusies en aanbevelingen van de evaluatie van DTC wordt in de komende jaren meer aandacht besteed aan bedrijven die een zekere mate van volwassenheid hebben ten aanzien van cybersecurity. Daarnaast stimuleert het DTC de totstandkoming van samenwerkingsverbanden onder meer om via dit netwerk kennis en best practices te delen. Voor het ontsluiten van informatie en advies voor meer volwassen bedrijven en voor de kennisdeling met en tussen de samenwerkingsverbanden en tussen grote en kleine bedrijven zal onder andere het door DTC ontwikkelde online platform worden gebruikt. **De leden van het CDA informeren of het NCSC vanuit de wettelijke grondslag enkel informatie over dreigingen en incidenten kan delen met CERTS of OKTT.** Het NCSC heeft, naast de primaire taak om Rijk en vitaal van bijstand bij dreigingen en incidenten te voorzien, ook tot taak om voor andere aanbieders relevante dreigingsinformatie, die het in het kader van die primaire taakuitoefening heeft verkregen te delen met andere CERTS of OKTT's, wanneer dit voor de doelgroepen van die organisaties relevante informatie betreft. Deze verstrekking kan, indien CERTS of OKTT's krachtens de de Wet beveiliging netwerk en informatiesystemen (Wbni) als zodanig zijn aangewezen, ook bepaalde vertrouwelijke dreigingsinformatie (bv. IP-adressen) betreffen. **De leden van de bovengenoemde fractie vragen zich vervolgens af of het feit dat het DTC niet is aangewezen als OKTT als een beperking gezien moet worden. Ook de leden van de VVD fractie vragen zich af waarom het DTC tot dusver nog niet is aangemerkt als OKTT en of ik bereid ben om de voorwaarden te scheppen waardoor dit wel mogelijk is** Om het NCSC in staat te kunnen stellen bijvangst, ook als het persoonsgegevens betreft, te kunnen delen met het DTC is inderdaad een aanwijzing als OKTT noodzakelijk. Momenteel wordt door het Ministerie van EZK gewerkt aan het voldoen van het DTC aan de voorwaarden waardoor het DTC krachtens de Wbni aangewezen kan worden als OKTT. Het is hierbij belangrijk om aan te geven dat de doelgroep van het DTC (niet-vitale bedrijfsleven) anders is dan die van het NCSC, de informatie van het NCSC zal niet in alle gevallen relevant zijn voor het DTC. Het DTC zal daarom naast de informatie die het van het NCSC ontvangt, ook andere informatiebronnen inzetten die goed aansluiten bij hun doelgroep. Het DTC heeft de ambitie een informatieknooppunt te zijn voor het niet-vitale bedrijfsleven, ook door informatie verkregen van de bedrijven zelf te ontsluiten voor andere bedrijven. **De bovengenoemde leden vragen of ik bereid ben het functioneren van het Digital Trust Center (DTC) verder te onderzoeken en daarin mee te nemen hoe, gegeven de omvang van het DTC en het MKB, het DTC een vertrouwde positie kan innemen richting miljoenen ondernemers?** Mijn collega van het Ministerie van EZK heeft zeer recent een externe evaluatie laten uitvoeren naar het functioneren van het DTC waaruit een aantal relevante aanbevelingen naar voren komen. Hierover is de kamer op 18 februari jl. geïnformeerd[26].Het Ministerie van EZK werkt aan de implementatie van deze aanbevelingen. Een deel van deze aanbevelingen heeft ook betrekking op het verbeteren van de relatie met en relevantie voor de brede doelgroep van het DTC.

De leden van D66 vragen hoe het kabinet aankijkt tegen de dubbele rol van verzekeringen (bijvoorbeeld bij randsomware) en of dit niet leidt tot meer cybercriminaliteit. Zoals ook geconstateerd

[26] Kamerstuk 26 643, nr.668

in de reactie op het WRR rapport kunnen verzekeringen een belangrijke rol spelen bij het helpen van partijen met schade om de draad weer op te pakken. Hoewel complex, ziet het kabinet wel dat schade na cyberincidenten steeds vaker onder normale bedrijfspolissen valt. Waar het gaat om cybercrime heb ik in reactie op vragen hiertoe van Lid Verhoeven (D66) en in de kamerbrief naar aanleiding van berichtgeving over Universiteit Maastricht[27] aangegeven dat het mijn voorkeur heeft dat de verzekeraar niet het losgeld vergoedt dat dan vervolgens in handen van criminelen terechtkomt, maar juist de geleden schade vergoedt door het niet betalen van dit losgeld. **De leden van D66 vragen mij ook hoe het staat met de uitvoering van de motie van de leden Verhoeven en Laan-Geselschap[28] over het scannen van overheidssystemen.** In de reactie op het WRR-rapport wordt gemeld dat door CIO-Rijk in overleg met de NCTV en het NCSC verkend wordt hoe rijksoverheidsorganisaties een doorlopende kwetsbaarhedenscan in kunnen richten. Dit overleg vindt op dit moment plaats. CIO-Rijk zal hier nog dit jaar een handreiking voor rijksoverheidsorganisaties voor opstellen.

4. COVID-19

De leden van de D66-fractie en GL-fractie maken zich zorgen over de impact van de Coronacrisis op cybersecurity. Urgentie van goed cybersecuritybeleid is verder toegenomen door de corona crisis. De leden willen weten welke gevolgen het kabinet hiervan ziet op het gebied van cybersecurity (cyberdreigingsniveau en hoeveelheid incidenten). Daarnaast vragen de leden van de GL-fractie of ik kan aangeven hoe ik zicht hou op deze ontwikkelingen en welke lessen hieruit kunnen worden geleerd om de beveiliging tegen cybercrime naar een hoger plan te tillen. Inzicht in de impact van de coronacrisis op cybersecurity is van groot belang en behoeft daarom goed de aandacht. Om in detail antwoord te kunnen geven zullen de vragen met betrekking tot de impact van de coronacrisis op cybersecurity worden beantwoord in de beleidsreactie Cybersecuritybeeld Nederland (CSBN) 2020 – voortgangsrapportage Nederlandse Cybersecurity Agenda (NCSA), die u begin juli zal toekomen.
De leden van de VVD-fractie en de CU-fractie vragen naar nieuwe ontwikkelingen op het gebied van cybercrime. En vragen of er een toename is voorzien van digitale aanvallen die samenhangen met signalen van personen die de huidige crisis rondom corona aangrijpen om bijvoorbeeld thuiswerkers te hacken, ziekenhuissystemen te ondermijnen of CEO-fraude te plegen. De leden vragen zich in het bijzonder af hoe dit wordt gemonitord en op welke wijze onze veiligheidsdiensten voorbereid zijn om hierbij snel op te treden. Op mijn verzoek ontvang ik periodiek een actueel beeld van de criminaliteit in deze periode van de crisis rond COVID 19. In mijn brief van 23 april 2020[29] bent u nader geïnformeerd. In deze brief is gemeld dat er sprake is van corona-specifieke criminaliteit – bijvoorbeeld phishing die inspeelt op corona of oplichting bij de verkoop van beschermende middelen – en van criminaliteitsvormen die juist toenemen. Zo is het aantal meldingen van online criminaliteit gestegen ten opzichte van dezelfde periode vorig jaar, waarbij overigens wel moet worden aangetekend dat ook voor de coronacrisis al sprake was van een toename. Op basis van de monitoring wordt met de betrokken partners gekeken of aanvullende interventies noodzakelijk zijn. Mede als gevolg van het

---

[27] Kamerstukken 26 643 en 28 684, nr.678
[28] Kamerstuk 30 821, nr. 85
[29] Brief van de bewindslieden van Justitie en Veiligheid van 23 april 2020 over de stand van zaken corona-maatregelen in de justitie, veiligheids- en migratieketen (Kamerstukken 35 300 VI en 25 295, nr. 126)

signaal dat online criminaliteit ten opzichte van dezelfde periode vorig jaar is toegenomen zijn al bestaande preventie-campagnes zoals *eerst checken, dan klikken* recent nog extra onder de aandacht van het publiek gebracht. Op 16 april is door het merendeel van de partners van het convenant *Eerst checken, dan klikken*, de Ministeries van BZK, een aantal waterschappen en gemeenten, ouderenbonden en jongerenplatform Scholieren.com aandacht besteed aan het risico van phishing. Hier is specifiek aandacht gevraagd voor phishing met betrekking tot corona. In deze berichtgeving is verwezen naar www.veiliginternetten.nl, waar een speciale pagina over internetveiligheid met betrekking tot corona is ingericht. Op 21 april 2020 heeft de politie de campagne *gamechangers* gestart waarbij speciale games moeten helpen jongeren uit de cybercriminaliteit te houden. **De leden vragen verder op welke wijze in internationaal verband hierbij wordt samengewerkt en hoe informatie wordt gedeeld om te voorkomen dat criminelen op grote schaal misbruik maken van de huidige crisis. Ze vragen hierbij welke concrete maatregelen worden genomen in internationaal verband om de uitwisseling van informatie te bevorderen? Daarnaast vragen de leden van de GL-fractie hoe de coördinatie van samenwerking tussen alle betrokken diensten, overheden, organisaties en bedrijven in de strijd tegen cyberaanvallen in coronatijd verloopt.** Binnen de EU heeft Europol ook enkele bevindingen gepubliceerd over criminaliteit in de COVID 19 periode[30]. De Nederlandse cijfers hebben met die bevindingen grote overeenkomsten. Binnen de beperkingen die de COVID-19 maatregelen voor politie en justitie met zich meebrengen, wordt nog steeds opgetreden tegen criminaliteit, waaronder cyber. De brief van 23 april 2020 bevat verder informatie over de wijze waarop de justitieketen zich steeds aanpast aan de ontwikkelingen in de omgang met de pandemie om zoveel mogelijk te blijven functioneren. Verder hebben de gevolgen van COVID-19 momenteel de volle aandacht van het Nationaal Cybersecurity Centrum (NCSC). Het NCSC werkt zo veel als mogelijk samen met het computercrisisteam van de zorgsector, genaamd Z-CERT. Samen met alle betrokken partijen, kijk ik continue welke inzet op het gebied van cybersecurity passend en nodig is. Het NCSC is ook lid van het Europese CSIRT-netwerk (Computer Security Incident Respons Teams) dat direct na het uitbreken van de COVID-19 crisis in verhoogde staat van paraatheid is gebracht waarbij de informatie-uitwisseling over significante cyberincidenten is geïntensiveerd en wekelijks situationele beelden met betrekking tot cybersecurity in de Europese lidstaten worden gedeeld.

De leden van de CDA-fractie vragen naar aanleiding van een radiouitzending naar een reactie op de conclusie van de journalisten dat ongeveer de helft van de in één week zeer fors toegenomen nieuw geregistreerde domeinnamen die gelinkt konden worden aan COVID-19 niet te vertrouwen is en zich waarschijnlijk bezighoudt met phishing. Zij vroegen verder naar mogelijkheden voor de Nederlandse overheid om actief te werken aan het uit de lucht halen van dergelijke websites. Phishing is een door criminelen veel gebruikte methode om personen te verleiden kwaadaardige software te activeren en om privé gegevens af te geven waardoor vervolgens personen slachtoffer worden van onder andere bankfraude, oplichting of gijzelsoftware. Het kabinet investeert daarom fors om internetcriminelen op te sporen. Dat is echter niet voldoende. Omdat internetcriminelen steeds handiger worden om toegang te krijgen tot computers, tablets en smartphones, is het belangrijk dat mensen zelf ook alerter online worden. Vorig jaar hebben mijn collega van EZK en ik en een groot aantal

[30] Europol heeft een monthly update gepresenteerd. Zie https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know

bedrijven en brancheorganisaties het convenant «Preventie cybercriminaliteit» ondertekend op grond waarvan wij samen optrekken in de strijd tegen internetcriminaliteit. Hiervoor wees ik al op door deze partners recent geïntensiveerde aandacht voor *eerst checken, dan klikken*. Tot slot wordt jaarlijks ook veel aandacht besteed aan de online gevaren in de campagne Alert Online.

De leden van de CDA-fractie vragen mij welke vormen van video-conferencing worden gezien als veilig en betrouwbaar en vragen of ik bereid ben om op korte termijn een waardering te geven voor de veelgebruikte video-conferencing applicaties. Of door een onafhankelijke organisatie hier onderzoek naar te laten doen. Aangezien veel mensen thuiswerken tijdens de COVID-19 uitbraak is het voor organisaties van belang dat zij kunnen beschikken over digitaal veilige applicaties voor video-conferencing. In de gevraagde behoefte van de Kamer is reeds voorzien. Om organisaties te helpen om een geïnformeerde keuze te maken, hebben organisaties zoals de Autoriteit Persoonsgegevens en Bits of Freedom vergelijkingen gepubliceerd die handvatten bieden. Daarnaast hebben het NCSC en het Digital Trust Centre (DTC) informatie en diverse adviezen gepubliceerd over veilig thuiswerken, waaronder over videobellen en online vergaderen[31]. **De leden van de CDA-fractie vragen of ik richtinggevende uitspraken kan doen naar overheidsorganen (landelijk en decentraal) om bepaalde video-conference-systemen of -applicaties niet te gebruiken.** Op basis van het Coördinatiebesluit Organisatie, Bedrijfsvoering en Informatiesystemen Rijksdienst kan de Minister van Binnenlandse Zaken na overleg met de andere Ministers gebruikskaders stellen, waarna er advies gegeven wordt over het gebruik van onveilige video-conference-systemen binnen de rijksdienst. Decentrale overheidsorganen nemen zelf deze beslissing op grond van hun lokale verantwoordelijkheid.

De leden van de D66-fractie vragen of ik van menig ben dat de coronacrisis noopt tot heroverweging van de aanwijzing van wat «essentiële diensten» zijn in het kader van de Wbni, bijvoorbeeld als het gaat om hosting- of datacenters. U bent bekend met het traject herijking vitaal. De corona-ervaringen worden hier zeker in meegenomen. Daarbij geldt dat ook wordt bezien of de nu nog niet als aanbieders van essentiële diensten c.q. vitale aanbieders aangemerkte aanbieders alsnog als zodanig moeten worden aangemerkt in het Bbni. Voor wat betreft de datacenters, bij de beantwoording van de Kamervragen van lid Van den Berg (CDA) heeft de Staatssecretaris van Economische Zaken en Klimaat toegezegd dat het kabinet voornemens is om nader onderzoek te doen naar de vraag of datacenters alsnog onderdeel moeten worden van de vitale infrastructuur.

De leden van GroenLinks hebben ook gevraagd naar de stappen die bijvoorbeeld zijn ondernomen tegen nep-RIVM-websites en tegen malware-aanvallen tegen ziekenhuizen die de afgelopen periode actief zijn geweest. Daarnaast vragen de leden of er voldoende capaciteit en expertise voorhanden is om te voorzien in een adequaat handhavingsniveau. Zoals hiervoor aangestipt, worden de ontwikkelingen in de criminaliteit in deze periode van de crisis rond COVID 19 goed gevolgd. Op basis van de monitoring wordt met de betrokken partners gekeken of aanvullende interventies noodzakelijk zijn voor corona-specifieke criminaliteit zoals bijvoorbeeld phishing die inspeelt op corona. De politie heeft in verband met de Coronacrisis al in een vroeg stadium actief contact gezocht met ziekenhuizen (Z-CERT) en is voor hen bereikbaar in het geval van cybercrime aanvallen. De politie

[31] https://www.ncsc.nl/onderwerpen/veilig-thuiswerken/videobellen-en-online-vergaderen

hanteert al een brede bestrijdingsstrategie met publieke en private partners in de aanpak van cybercrime, met naast opsporing aandacht voor alternatieve interventies zoals preventie en verstoring. Deze wordt ook voor de actuele dreiging ingezet. Mijn handelen is er onder andere op gericht om preventie te versterken en de weerbaarheid van de samenleving te vergroten. Dat gebeurt niet alleen met publieke organisaties maar ook met private partijen, bijvoorbeeld zoals verenigd in het convenant *Eerst checken, dan klikken*. Recentelijk, afgelopen 16 april, is door een groot aantal organisaties aandacht geschonken aan voorkoming van slachtofferschap van cybercriminaliteit. In dit verband wijs ik graag op de website www.veiliginternetten.nl. Daarnaast bespreken de verantwoordelijke teams van de politie ten aanzien van cybercrime wekelijks de ontwikkelingen om hier in de aanpak op in te spelen en in geval van aangifte onderzoek naar te doen.

De leden van de GL-fractie en de leden van de CU-fractie vragen mij of ik kan toelichten hoe vanuit het kabinet is bijgedragen aan de veiligheid en beveiliging van thuiswerkers met cruciale beroepen en de veiligheid van burgers in de digitale wereld. Het toenemende gebruik van digitale technologie tijdens de crisis heeft ervoor gezorgd dat de risico's voor burgers en bedrijven zijn toegenomen. De huidige crisis heeft het belang van goede voorlichting over cybersecurity verder onderstreept. Het DTC heeft op haar website diverse pagina's gewijd aan veilig thuiswerken, veilig video-bellen en het beveiligen van je thuisnetwerk. Het DTC heeft hierover ook zijn doelgroep geïnformeerd. Daarnaast heeft op 16 april het merendeel van de partners van het convenant *Eerst checken, dan klikken*, naast verscheidene andere partners zoals het Ministerie van BZK, een aantal waterschappen en gemeenten, ouderenbonden en een jongerenplatform aandacht besteed aan het risico van phishing. Daarbij is speciale aandacht besteed aan phishing met betrekking tot corona. Het betreft vooral uitingen op social media, waarbij is verwezen naar www.veiliginternetten.nl. Daar is een speciale pagina over internetveiligheid met betrekking tot corona ingericht. Daarnaast zijn ook publieke adviezen, o.a. over thuiswerken en online vergaderen, van het NCSC raadpleegbaar op de NCSC-website.

De leden van de CU-fractie vragen mij of een vrijwillige deelname aan de Corona-apps niet een harde eis behoort te zijn in plaats van een uitgangspunt. Met verwijzing naar de brief van de Minister van VWS van 21 april 2020[32]. kan ik aangeven dat momenteel wordt verkend welke apps binnen een beleid van testen, traceren en thuisrapportage kunnen worden ingezet. Cruciale randvoorwaarden zijn privacy (inclusief dataprotectie), informatieveiligheid, grondrechten, nationale veiligheid en toegankelijkheid. Vrijwilligheid is geen eis aan de apps maar aan de inzet. Inzet van een app zal vrijwillig zijn**. De leden vragen of naast commerciële partijen ook universiteiten en academische instellingen bij de uitwerking van de Corona-apps worden betrokken.** De inzet is om te beschikken over een team met de juiste bouwers en ook met experts waaronder deskundigen van universiteiten en academische instellingen, van onder andere informatieveiligheid, privacy, grondrechten, nationale veiligheid en inclusie. **Tot slot vragen de leden of de Data Protection Impact Assessment van de uiteindelijke applicaties openbaar worden gemaakt ten behoeve van het maatschappelijk vertrouwen.** Hierover kan ik zeggen dat tenminste een samenvatting van de Data Protection Impact Assessment openbaar gemaakt zal worden. De Minister van VWS streeft naar volledige openbaarmaking als andere belangen dat niet in de weg staan zoals het openbaar maken van gevoelige bedrijfsinformatie.

[32] Kamerstuk 25 295, nr. 277

De leden van de CU-fractie en de CDA-fractie vragen mij op welke wijze coördinatie van de cybersecurity in de zorgsector plaatsvindt met zorgpartijen en welke inspanningen er worden geleverd om ons internet stabiel en veilig te houden. De leden vragen of hierbij aandacht is voor de kleinere zorginstellingen en of de urgentieverklaring van de Cyber Security Raad (CSR) hierbij wordt betrokken. Om de verspreiding van COVID-19 tegen te gaan werken veel mensen thuis. Ook is het extra belangrijk dat de zorg zijn werk kan uitvoeren zoals normaal en niet verstoord wordt door bijvoorbeeld digitale aanvallen, zoals ook door de CSR benoemd. Beide aspecten hebben geleid tot extra maatregelen om de digitale weerbaarheid te verhogen. Het NCSC heeft een COVID-19 dossier op zijn website gepubliceerd met relevante adviezen, onder andere over hoe je veilig kan thuiswerken. Het computercrisisteam voor de Zorg, Zorg-CERT, werkt nauw met het NCSC samen om de digitale weerbaarheid van ziekenhuizen te verhogen. Zo deelt het NCSC waar mogelijk voor de zorg relevante incident- en dreigingsinformatie met Z-CERT. Z-CERT kan hierdoor analyses maken en de zorgsector van adviezen voorzien. Als er zich een incident voordoet met aanzienlijke gevolgen voor de continuïteit van een zorginstelling, kan het NCSC – bij een vrijwillige melding van de zorginstelling – ook rechtstreeks aan die instelling bijstand verlenen. Alle betrokken partijen kijken continue welke eventueel aanvullende inzet op het gebied van cybersecurity passend en nodig is. **De leden van de CDA-fractie en GL-fractie willen weten of ik bekend ben met de private initiatieven en samenwerkingsverbanden om de overheid en met name de zorg te ondersteunen. De leden willen weten of het ministerie gebruikt maakt van deze initiatieven en welke kansen en risico's ik voorzie in de samenwerking op cybersecurity tussen publiek en private organisaties. Daarnaast vragen de leden welke mogelijkheden ik zie om zorginstellingen te wijzen op het initiatief: wijhelpenziekenhuizen.nl, waarbij bedrijven zorginstellingen helpen op het gebied van cybersecurity**. Publiek-private aanpak van cybersecurity is een belangrijk onderdeel van de Nederlandse cybersecurity aanpak. Ik verwelkom daarom het private initiatief «wijhelpenziekenhuizen». Dit initiatief is via diverse kanalen onder de aandacht gebracht van de zorginstellingen in Nederland. Z-CERT heeft met betrekking tot dit initiatief een coördinerende en verbindende rol door vraag en aanbod bij elkaar te brengen.

De leden van de CU-fractie vragen mij of ik kan aangeven in hoeverre de vernielingen van zendmasten risico met zich meebrengen voor de netwerkcapaciteit, juist nu we zoveel vanuit huis werken en gebruik maken van videobellen. De telecomnetwerken in Nederland zijn van hoge kwaliteit en juist in deze tijden nog meer dan anders van groot belang, omdat ze mede mogelijk maken dat we veilig thuis kunnen werken. De netwerken worden op dit moment anders belast dan normaal. Zo wordt er meer mobiel gebeld en is er meer dataverkeer vanaf particuliere internetaansluitingen en minder vanuit kantoren. Er is gemiddeld in Nederland ruim voldoende capaciteit in zowel mobiele als vaste verbindingen**. De leden vragen daarnaast wat de gevolgen zijn voor de nationale veiligheid gezien de zendmasten onderdeel zijn van de kritieke nationale infrastructuur en of er al een aanleiding is om de beveiliging van de zendmasten op te schalen om de leveringszekerheid te kunnen borgen.** De risico's voor de nationale veiligheid zijn op landelijke schaal beperkt. Er zijn in Nederland 18.789 geregistreerde antenne-installaties. Regionaal kunnen er door brandstichting wel risico's ontstaan, afhankelijk van welke installaties worden getroffen en hoeveel tijd nodig is om de dienstverlening te herstellen. Brandstichting in zendmasten kan leiden tot een verlies van capaciteit in het mobiele netwerk in de directe omgeving

van de zendmast. Dit kan zich bijvoorbeeld uiten in langzamere mobiele verbindingen. In veel gevallen kunnen omliggende zendmasten het verkeer overnemen tot de zendmast is hersteld. In het ergste geval zijn één of meerdere masten in een gebied tijdelijk niet beschikbaar, en kan ook een storing in de continuïteit van het netwerk optreden als er geen dekking is in de directe omgeving van de zendmast. Dan is tijdelijk géén of een slechtere verbinding mogelijk, met als belangrijkste risico dat burgers 1-1-2 niet tijdig kunnen bereiken, of een NL-Alert niet ontvangen.
Naast zendmasten zijn ook 1-1-2 en C2000 onderdeel van de kritieke (vitale) nationale infrastructuur. Op de bereikbaarheid van 1-1-2 hebben de branden vooralsnog mogelijk in ten minste één geval in één geval impact gehad. Dit heeft voor zover bekend niet geleid tot persoonlijke ongevallen. Het risico op verminderde bereikbaarheid van 1-1-2 is normaliter beperkt. Wanneer er in een gebied geen dekking is van de eigen mobiele operator, schakelt de mobiele telefoon voor een noodoproep aan 1-1-2 automatisch over op een andere provider. Indien de fysieke afstand tot de vervangende mast te groot is, bestaat echter de kans dat 1-1-2 via mobiele telefonie onbereikbaar is. De operationele impact van de branden voor C2000 is vooralsnog beperkt. Alle C2000-masten zullen de komende periode extra beveiligd worden.
Het Ministerie van EZK staat in nauw contact met de sector, het Ministerie van JenV en de Landelijke Eenheid van de politie om te bezien in hoeverre aanvullende maatregelen noodzakelijk zijn en welke vorm deze maatregelen aan kunnen nemen. **De leden van de CU-fractie vragen of ik bereid ben om sociale media platforms aan te spreken op hun verantwoordelijkheid om valse berichtgeving tegen te gaan die aan kan zetten tot deze daden van brandstichting.** Vanuit de overheid is er regelmatig contact met Tech bedrijven, mede in de context van de uitvoering van de Europese gedragscode over desinformatie. De rol die zij spelen in het bestrijden van desinformatie in algemene zin en de specifieke mis- en desinformatie rondom COVID-19 en 5G zijn uiteraard onderwerp van gesprek. Ook de Europese Commissie spreekt de bedrijven geregeld aan op de maatregelen die zij nemen, ook in de context van COVID-19. **Tot slot willen de leden weten of er wordt samengewerkt met andere overheden, waaronder het VK, om verspreiding van complottheorieën tegen te gaan**. Zoals ik u ook heb aangegeven in reactie op de vragen tijdens het SO Nationale veiligheid, wisselt Nederland continu informatie uit met partners in EU- en NAVO-verband en bilateraal, ook op dit soort problematiek. In deze contacten worden analyses en beleidsaanpak gedeeld. Daarbij heeft Nederland uiteraard extra aandacht voor landen waar deze kwestie ook speelt.»

Ten aanzien van cybercriminaliteit vragen de leden van de CU-fractie voorts welke ontwikkelingen zichtbaar zijn in gedwongen prostitutie via het darkweb en apps als telegram. Wat is de stand van zaken in de opsporing? Hoe vaak is het afgelopen jaar gebruik gemaakt van de webcrawler? Wordt, sinds de afkondiging van een verbod op contactberoepen en de sluiting van seksinrichtingen, een toename geconstateerd van prostitutie-advertenties op genoemde kanalen? Wordt daar vervolgens ook op gehandhaafd? Sinds de afkondiging van het verbod op contactberoepen en de sluiting van seksinrichtingen, wordt een afname van prostitutieadvertenties gezien waarin fysieke seksuele diensten worden aangeboden. Wel is er een toename te zien van platformen die webcamsex aanbieden. De landelijk officier mensenhandel heeft, in afstemming met de G4-gemeenten, Groningen en Nijmegen en in samenspraak met het Ministerie van Justitie en Veiligheid, alle in Nederland actieve platform nogmaals gewezen op de noodverordening, inclusief de maatregel dat fysiek contact verboden is, en hen hierbij ook

gewezen op hun maatschappelijke verantwoordelijkheid. Er worden vanuit de gemeente, in samenspraak met de politie, controles gedaan op die advertenties. Naast open bronnenonderzoek, wordt er ook gekeken naar de mogelijkheden om webcrawling technologie in te zetten t.b.v. de opsporing van mensenhandel. Hiertoe wordt door politie en OM gewerkt aan een juridisch handelingskader.

5. Overig

De leden van de CDA-fractie vragen zich af hoe de extra inspanningen (ruim € 20 miljoen) op kennis & innovatie zich verhouden tot investeringen in andere landen en welke soortgelijke investeringen in landen als Duitsland en Frankrijk worden gedaan? Het is lastig om deze landen met elkaar te vergelijken onder meer door verschillen in de rol van de centrale overheid, verschillen in de aanpak van kennisontwikkeling & innovatie en de wijze waarop investeringen gedaan worden (instrumenten). In Frankrijk zijn er verschillende ministeries en instanties betrokken bij de investeringen in cybersecurity. In Frankrijk bedragen investeringen door de centrale overheid ongeveer 230 miljoen per jaar, waarvan bijvoorbeeld grofweg de helft naar een grootschalig cyberprogramma gericht op het aannemen van «cyber-soldaten» (militair personeel met specialisatie op cybersecurity) gaat. Voor Duitsland is het verhaal ingewikkelder: meerdere ministeries houden zich met cybersecurity bezig en hebben een verscheidenheid aan instituten, initiatieven en strategieën ontwikkeld. Kennisontwikkeling en innovatie is een onderdeel van hun investeringen waarbij ieder ministerie, instituut en deelstaat vaak een eigen R&D budget heeft. Op federaal niveau is er naar schatting 108 miljoen beschikbaar, daarnaast zijn er per deelstaat wisselende hoeveelheden beschikbaar. Door de grote hoeveelheid aan spelers is het moeilijk om de totale omvang van de investeringen in één getal samen te vatten. Bovendien spelen factoren als inwonertal, grootte van de economie en autonomie van verschillende overheden hierbij een rol. Het Nederlandse beleid is juist gericht op het samenbrengen van de verschillende initiatieven en spelers. Nederland investeert daarbij op een andere manier in kennis & innovatie dan veel omringende landen. Grote nadruk ligt op (generieke) bottom-up instrumenten en een sterke verankering in publiek-private samenwerking. Dat is ook de opzet van de kennis- en innovatie-agenda Veiligheid, missie cyberveiligheid, één van de instrumenten die zal vallen onder het nieuwe samenwerkingsplatform waar uw Kamer per brief van 9 april 2020 is geïnformeerd door de Staatssecretaris van EZK, mede namens onder andere mijzelf. Dit instrument richt zich op duurzame samenwerking tussen publieke en private partijen over de hele keten heen. Via het nieuwe samenwerkingsplatform proberen we middelen, instrumenten en kennis binnen het cybersecuritydomein zo effectief mogelijk te bundelen en te benutten op het gebied van onderzoek, onderwijs en innovatie. **De leden vragen vervolgens of de Nederlandse investeringen voldoende zijn om toptalent en topkennis aan ons land te binden?** Tijdens het Algemeen Overleg AI en Sleuteltechnologie in maart jl., heb ik uw Kamer toegezegd om na te gaan welke factoren er zoal spelen rond het behouden van talent in Nederland. Daarbij kijken we ook of de aanwezigheid van voldoende middelen een rol speelt in de keuze om in Nederland te blijven of niet. Ik zal uw Kamer daar voor de zomer over informeren.

De leden van D66 en de VVD stellen verschillende vragen over de evaluatie van de NCSA en het onderzoek naar waar meer investeringen nodig zijn. In mijn brief over de het WRR-rapport en de evaluatie rondom de Citrix-problematiek kondigde ik aan dat de Cyber Security Raad een brede evaluatie van de aanpak van cybersecurity zal verrichten. Na overleg met de Raad is besloten dat zij een advies uitbrengen over

investeringen die nodig zijn in cybersecurity voor het volgende kabinet[33]. Met het oog op de voorbereidingen hiervoor is de CSR verzocht om haar advies voor 15 december 2020 uit te brengen. Parallel hieraan zal bij het Wetenschappelijk Onderzoek en Documentatie Centrum (WODC) een verzoek worden uitgezet voor het verrichten van de evaluatie van de Nederlandse Cyber Security Agenda (NCSA), zoals toegezegd bij verzending van de NCSA aan de Kamer in april 2018. Dit dient een brede evaluatie te worden die de inspanningen van de overheid binnen de zeven ambities van de NCSA omvat. Binnen dit evaluatieonderzoek kunnen eerdere rapporten over specifieke aspecten van de Nederlandse cybersecurityaanpak, zoals de onderzoeken van de Algemene Rekenkamer waar de leden van de VVD aan refereren, worden meegenomen. De evaluatie van de NCSA zal in de loop van 2021 worden afgerond.

[33] Hiermee geef ik invulling aan de toezegging tijdens het AO-Cybersecurity 30 oktober 2019 (op verzoek van Kamerlid Verhoeven D66) om te bezien waar in de toekomst meer investeringen nodig zijn. Kamerstuk 26 643.