2020D14822

INBRENG VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

De vaste commissie voor Justitie en Veiligheid heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Justitie en Veiligheid 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» (Kamerstuk 26 643, nr. 673).

De voorzitter van de commissie,
Van Meenen

De adjunct-griffier van de commissie,
Burger

Inhoudsopgave **Blz.**

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-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-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-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 vertrouwens-persoon 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- Verhoeven/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 urgentie-verklaring 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 thuis-werken, 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 werkzaam-heden. 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