

Vergaderjaar 2017–2018

25 124

Nieuwe infrastructuur mobiele communicatie (C2000)

Nr. 90

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 5 juli 2018

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 26 april 2018 over de voortgang van C2000 en alarmnummer 112 (Kamerstuk 25 124, nr. 89).

De vragen en opmerkingen zijn op 5 juni 2018 aan de Minister van Justitie en Veiligheid voorgelegd. Bij brief van 3 juli 2018 zijn de vragen beantwoord.

De voorzitter van de commissie,
Van Meenen

Adjunct-griffier van de commissie,
Verstraten

| | | |
|------------|---|----------|
| I. | Vragen en opmerkingen vanuit de fracties | 2 |
| 1. | Inleiding | 2 |
| 2. | Vernieuwing C2000 systeem | 2 |
| 3. | Continuïteit huidige C2000 systeem | 4 |
| 4. | Financiële consequenties | 6 |
| 5. | Toekomstig mobiel breedband voor de OOV-diensten | 6 |
| 6. | Nieuwe meldkamers | 7 |
| 7. | Stand van zaken 112 | 7 |
| II. | Reactie van de Minister van Justitie en Veiligheid | 8 |

I. Vragen en opmerkingen vanuit de fracties

1. Inleiding

De leden van de VVD-fractie hebben kennisgenomen van de brief inzake de voortgang C2000 en 112 (Kamerstuk 25 124, nr. 89, hierna: uw brief). Zij hebben hierover enkele vragen.

De leden van de CDA-fractie hebben met interesse kennisgenomen van de brief over C2000 en 112. Zij hebben tevens naar aanleiding van de uitzending van Zembla van woensdag 16 mei 2018, nog een aantal vragen.

De leden van de D66-fractie hebben enkele vragen.

De leden van de SP-fractie hebben enkele vragen.

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van de brief. Tevens hebben zij kennisgenomen van de tv-uitzending van Zembla van 16 mei 2018 over C2000. Zij hebben de volgende vragen.

De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van de brief. Zij hebben op enkele punten behoefte aan een nadere toelichting.

2. Vernieuwing C2000 systeem

De leden van de VVD-fractie constateren dat u op 15 mei 2018 heeft aangegeven, met het oog op nationale veiligheid, te stoppen met het gebruik van antivirussoftware van Kaspersky Lab, een Russisch bedrijf. Kunt u aangeven waarom Nederland met een Russisch antivirussoftware-bedrijf geen zaken kan doen, maar het communicatienetwerk van onze hulp- en veiligheidsdiensten wel door een Chinees bedrijf (Hytera) ingericht kan worden?

De leden van de CDA-fractie vragen wat thans de exacte implementatiedata zijn per regio/meldkamer en vragen u dit te specificeren voor zowel de implementatie van het nieuwe spraaknetwerk (koppeling aan de huidige radiobediening in de meldkamers) als voor de (in 2019 voorziene) koppeling van de nieuwe radiobediening aan het vernieuwde spraaknetwerk.

De aan het woord zijnde leden vragen of u nog steeds van mening bent dat de drie bij de vernieuwing van C2000 betrokken marktpartijen in staat zijn om het door hen aangenomen werk daadwerkelijk binnen een redelijke termijn uit te voeren. Kunt u hierbij specifiek ingaan op de verwachtingen ten aanzien van Hytera Mobilfunk GmbH, mede gelet op hetgeen in de Zembla-uitzending ten aanzien van deze firma naar voren is gebracht?

De voornoemde leden vragen of het klopt dat Hytera Mobilfunk GmbH een Duitse dochteronderneming is van het Chinese bedrijf Hytera Communications. Klopt het dat de Algemene- en Militaire Inlichtingen en Veiligheidsdienst (hierna: AIVD/MIVD) ernstige bezwaren hebben tegen de betrokkenheid van een Chinese partij bij de bouw van C2000? Deze leden vragen of u, mede in het licht van regeringsopstelling ten opzichte van Kaspersky, kunt uitleggen hoe u nu tegen deze situatie aankijkt. Is het nodig dat aanvullende maatregelen worden genomen om risico's in te perken?

De voornoemde leden vragen of u de lijst met 30 dekkingsissues aan de Kamer kunt doen toekomen, dan wel vertrouwelijk ter inzage leggen.

De leden van de D66-fractie merken op dat de vernieuwing van C2000 nu al enkele jaren gaande is. Kunt u een overzicht bieden van de stappen die de afgelopen jaren zijn gezet in de vernieuwing van C2000? Kan daarbij worden aangegeven op welke momenten – en met welke reden – vertraging is opgelopen?

De voornoemde leden lezen dat de afgelopen jaren vorderingen zijn gemaakt in het oplossen van dekkingsissues, maar dat deze nog niet volledig verholpen zijn. Hoeveel staan hiervan momenteel nog open? Wat is de gemiddelde looptijd waarin dekkingsissues opgelost worden? Hoe varieert de looptijd in het oplossen van een dekkingsissue met hoge versus lage prioriteit? Op welke wijze wordt bepaald dat dekkingsissues op bepaalde plekken lage prioriteit genieten? Hoe sluit u uit dat in dergelijke gebieden grote calamiteiten plaatsvinden waarvoor toereikende dekking van C2000 wel degelijk noodzakelijk is? Kunt u tenslotte de meest recente versie van de Dekkings Issue Prioriterings Procedure-lijst (hierna: DIPP-lijst) aan de Kamer doen toekomen? Bent u bereid updates van deze lijst periodiek aan de Kamer te doen toekomen? Zo nee, waarom niet?

De aan het woord zijnde leden merken op dat de hoofdleverancier van het nieuwe C2000 systeem Hytera Mobilfunk GmbH is, een dochterorganisatie van het Chinese hightechbedrijf Hytera Communication, dat goede zakelijke betrekkingen onderhoudt met de Chinese overheidsdiensten. Is dit waar? Zo ja, acht u het verantwoord om een voor de Nederlandse veiligheid essentieel missiekritisch netwerk aan een Chinese partij te gunnen? Zo ja, hoe verhoudt zich dit tot uitspraken van de AIVD-directeur eerder dit jaar, waarin hij stelt dat China tot één van de drie grootste bedreigingen voor de cyberveiligheid behoort, aangedreven door de overheid? Waarop baseert u de stelling dat C2000 een voor hackers «onneembare vesting» is, zoals gesteld in de voornoemde Zembla-uitzending.

De leden van de PvdA-fractie constateren dat in de voornoemde uitzending van Zembla wordt gemeld dat de AIVD en MIVD zorgen hebben over het feit dat een Chinees bedrijf betrokken is bij de bouw van C2000. De aan het woord zijnde leden vragen of deze zorgen bij u reeds bekend waren. Zo ja, vanaf welke datum? Wat heeft u naar aanleiding van deze waarschuwing gedaan? Was Hytera ten tijde van de aanbesteding al in Chinese handen? Zo ja, speelde bij het toekennen van de opdracht mee dat het bedrijf in Chinese handen was? Zo nee, zou u, mocht u op dat moment hebben geweten dat Hytera in Chinese handen zou komen, de opdracht ook hebben gegund of mogelijk aanvullende voorwaarden hebben gesteld? Wat kunt u nu nog doen om te voorkomen dat dit deel van de vitale infrastructuur van C2000 door sabotage vanuit China wordt bedreigd?

Deelt u de mening van de directeur van de AIVD dat er in zijn algemeenheid vanuit China sprake is van cyberdreiging? Zo ja, acht u de dreiging van sabotage van C2000 door China een reële dreiging? Zo nee, waarom niet?

De leden van de ChristenUnie-fractie constateren dat in de grensregio het knelpunt bestaat dat samenwerkende Veiligheidsregio's in Nederland, Duitsland en België verschillende communicatiesystemen in de voertuigen (zoals de brandweerauto's) hanteren, waardoor snelle en directe communicatie wordt bemoeilijkt bij calamiteiten. Zeker bij een grote calamiteit moeten politie, brandweer en ambulancediensten kunnen vertrouwen op directe en ongehinderde communicatie. De voornoemde leden vragen op welke manier rekening wordt gehouden met samenwerkende Veiligheidsregio's in de grensregio bij het huidige C2000-systeem en bij de verdere ontwikkeling van het C2000-systeem. Hoe wordt nu en in de toekomst directe en ongehinderde communicatie gegarandeerd tussen de Nederlandse, Duitse en Belgische hulpverleningsdiensten?

3. Continuïteit huidige C2000 systeem

De leden van de VVD-fractie lezen dat het huidige C2000 systeem zich heeft ontwikkeld tot een robuust en stabiel systeem. In de uitzending van het televisieprogramma Zembla op 16 mei 2018 wordt echter op basis van een interne memo van de politie gemeld dat het huidige systeem steeds vaker met storingen kampt, 2775 tussen april 2015 en augustus 2017. Kloppen de getallen die Zembla noemt? Zo ja, hoe kan u een dergelijk aantal storingen rijmen met een robuust systeem? Bij hoeveel storingen vindt u C2000 niet meer robuust?

In de uitzending van Zembla wordt tevens gemeld dat een derde van de 2775 storingen het gevolg waren van een defect onderdeel, terwijl reserve-onderdelen voor het oude systeem moeilijk of niet meer verkrijgbaar zijn. Klopt het dat Motorola en KPN, de leveranciers van C2000, hebben aangegeven dat de stabiliteit van C2000 na 2018 alleen gewaarborgd kan worden als er forse technologische updates plaatsvinden? Zo ja, op welke manier is geborgd dat die noodzakelijke updates plaatsvinden nu Motorola en KPN vanaf 2019 niet meer betrokken zijn bij C2000? Op welke wijze kunnen de partijen die het beheer over C2000 vanaf januari 2019 over moeten nemen de stabiliteit van C2000 waarborgen?

In uw brief staat dat de audits op het huidige C2000 die aan de basis staan van het oordeel dat C2000 robuust en stabiel is uitgevoerd zijn door Xebia. Klopt het dat Xebia ook de audits op het nieuwe C2000 uitvoert? Deelt u de mening dat het wenselijk is dat een partij die geen betrokkenheid heeft bij het nieuwe C2000 een dergelijke audit uitvoert? Zo ja, bent u, mede op basis van de bevindingen van Zembla, bereid een nieuwe audit uit te laten voeren? Zo nee, waarom niet?

U schrijft tevens dat onderhoud aan het systeem en aanvulling van reserve-onderdelen onderdeel waren van de uitvraag aan leveranciers. Klopt het dat deze onderdelen niet meer gemaakt of geleverd worden nu Motorola de ontwikkeling en het onderhoud van C2000 heeft gestaakt? Kunt u aangeven hoe een leverancier een reserve-onderdeel kan aanleveren dat niet meer gemaakt wordt? Deelt u de mening dat het een veiligheidsrisico met zich meebrengt wanneer gewerkt wordt met verouderd materiaal waarvoor geen reserve-onderdelen meer beschikbaar zijn?

U beschrijft contractuele afspraken en maatregelen die de continuïteit van het huidige C2000 systeem moeten waarborgen. Kunt u op basis van de gemaakte contractuele afspraken garanderen dat het huidige C2000, indien dat in 2019 nog gebruikt moet worden, accuraat blijft functioneren, ook in geval van zwaar gebruik, zoals bijvoorbeeld het geval kan zijn na een terroristische aanslag?

De leden van de CDA-fractie vragen of u de in het programma Zembla naar voren gebrachte stelling onderschrijft dat het huidige C2000 steeds storingsgevoeliger wordt en dat vervangingsonderdelen – ook voor

bijvoorbeeld portofoons – nauwelijks meer te verkrijgen zijn? Deze leden vragen of u kunt uiteenzetten met welke firma's een contract is gesloten om het functioneren van het huidige C2000 – in brede zin – na 2018 te kunnen continueren.

De voornoemde leden vragen de door u genoemde audits van onderzoeksbureau Xebia aan de Kamer kan doen toekomen, dan wel vertrouwelijk ter inzage te leggen.

De leden van de D66-fractie lezen dat het huidige C2000 systeem zich de afgelopen jaren heeft ontwikkeld tot «een systeem dat zich robuust en stabiel gedraagt». Uit welk onderzoek is dit gebleken? Kunt u dit onderzoek aan de Kamer doen toekomen? Zo nee, waarom niet? Kunt u een overzicht geven van het aantal storingen met het huidige C2000 systeem in de afgelopen vijf jaar, uitgesplitst per maand? Klopt het dat het huidige C2000 systeem steeds meer storingen ondervindt? Zo ja, hoe verhoudt zich dit tot de stellingname dat het huidige C2000-systeem zich de afgelopen jaren heeft ontwikkeld tot een «systeem dat zich robuust en stabiel gedraagt»?

De leden van de D66-fractie vragen of het klopt dat sommige recherche-teams van de politie alternatieve communicatiemiddelen aanschaffen omdat het vertrouwen in het C2000 systeem te ver is afgenomen, zoals is gesteld in de voornoemde Zembla-uitzending? Zo ja, hoe verhoudt zich dit tot de stellingname dat het huidige C2000 systeem zich de afgelopen jaren heeft «ontwikkeld tot een robuust systeem waar de hulpverleningsdiensten op kunnen vertrouwen»?

Bent u bekend met het geciteerde document uit de voornoemde Zembla-uitzending waaruit blijkt dat bij een grote calamiteit zoals een terroristische aanslag het C2000 systeem niet toereikend is om alle (gelieerde) gebruikers toe te laten tot het communicatiesysteem? Klopt het dat hierin wordt gesteld dat «in het geval van een aanslag, de communicatiesystemen overbelast [kunnen] raken doordat de vraag naar de gespreks capaciteit het aanbod overstijgt»? Klopt het dat op dit moment niet alle relevante gelieerde organisaties (zoals ziekenhuizen, de Reddingsbrigade en huisartsenposten) niet meer worden toegelaten op het C2000 systeem? Zo ja, op basis van welke afspraken wordt bepaald welke organisaties wel en niet toegang krijgen tot het communicatiesysteem? Hoe wordt dit naar de betreffende organisaties gecommuniceerd? Deelt u de mening dat dergelijke keuzes grote risico's voor de veiligheid met zich mee kunnen brengen? Kunt u het door Zembla geciteerde document aan de Kamer doen toekomen? Zo nee, waarom niet? Waarop baseert u voorts de stellingname uit uw reactie op de uitzending (<https://www.rijksoverheid.nl/actueel/nieuws/2018/05/16/reactie-naar-aanleiding-van-uitzending-zembla-over-c2000>) dat «ervaringen uit het buitenland hebben aangetoond dat in het geval van een aanslag de gebruikte communicatiesystemen overbelast kunnen raken doordat de vraag naar gespreks capaciteit het aanbod overstijgt»? Bij welke incidenten heeft zich dit in het buitenland voorgedaan en op welke wijze zijn deze vergelijkbaar met de werking van C2000?

Klopt het dat u bij de aanbesteding van het nieuwe C2000 systeem heeft gekozen voor de meest goedkope optie door de aanbesteding te gunnen aan een drietal leveranciers (Hytera Mobilfunk GmbH, 2Way en Eurofunk)? Kunt u de andere kandidaten en de bijbehorende offertes voor de aanbesteding van het nieuwe C2000 systeem aan de Kamer doen toekomen? Zo nee, waarom niet?

Klopt het dat het Ministerie van Justitie en Veiligheid iedereen die meewerkt aan C2000 verboden heeft om met Zembla te spreken naar aanleiding van de uitzending over C2000? Zo ja, waarom?

De leden van de PvdA-fractie merken op dat in de voornoemde Zembra-uitzending wordt gesteld dat bij een grote calamiteit of een terroristische aanslag het communicatienetwerk C2000 overbelast kan raken. Herkent u dit probleem? Zo ja, wat heeft u gedaan om dit probleem op te lossen? Zo ja, had de Kamer eerder kennis van dit probleem kunnen nemen en wanneer dan? Is er sprake van een noodplan? Zo ja, wat houdt dit in? Zo nee, waarom is er geen noodplan? Is het waar dat na een groot incident het mogelijk is dat alleen een beperkte groep gebruikers voorrang op het spraaknetwerk krijgt en dat voor andere gebruikers de kans bestaat dat communicatie via C2000 niet meer mogelijk is? Zo ja, welk soort gebruikers zou dan geen gebruik meer kunnen maken van C2000? Is het waar dat daar bijvoorbeeld de kerncentrale in Borssele, huisartsenposten of reddingsbrigades toe kunnen behoren? Welke risico's brengt dit met zich mee?

Tot wanneer kan het bestaande C2000 in technische zin volledig operationeel blijven? Is het waar dat het onderhoudscontract tot eind 2019 loopt? Is er dan sprake van een volledig operationeel nieuw systeem? Op basis van welk extern onderzoek blijkt dat het huidige C2000 systeem nog robuust en betrouwbaar is? Is dat onderzoek openbaar? Zo ja, waar kan het dan gevonden worden? Zo nee, waarom niet? Kan het – desnoods in vertrouwen – met de Tweede Kamer gedeeld worden?

De leden van de SP-fractie maken zich zorgen over de aanhoudende berichten dat er bij een grote crisis zoals een terroristische aanslag het netwerk van C2000 niet zal voldoen. De voornoemde leden vragen of u kan verzekeren dat ook bij grote drukte op het netwerk, het netwerk nog wel functioneert. Juist op dat soort momenten is het immers van belang dat de diensten goed met elkaar kunnen communiceren. Als dit niet waar te maken is, wat zijn dan de alternatieven en bent u bereid dat te onderzoeken? De voornoemde leden verzoeken een overzicht van de totale kosten van C2000 tot nu toe, inclusief wat er eerst geraamd was.

De leden van de ChristenUnie-fractie lezen dat het C2000 systeem zich de afgelopen jaren heeft ontwikkeld tot een robuust systeem waar de hulpverleningsdiensten op kunnen vertrouwen. Uitgangspunt is dat het nieuwe C2000 systeem pas in gebruik genomen wordt als het aan deze zelfde robuustheid voldoet.

De aan het woord zijnde leden verzoeken u in dit licht te reageren op de berichten dat bij grote calamiteiten zoals een terroristische aanslag, het C2000 communicatienetwerk overbelast kan raken. Hoe robuust is de dekking van het systeem? Vanaf welk moment was er volgens u sprake van een robuust systeem? Welke lessen heeft u geleerd van de ontwikkeling van het huidige systeem?

4. Financiële consequenties

De leden van de CDA-fractie vragen of u explicieter inzichtelijk kunt maken welke incidentele extra uitgaven gedaan moeten worden en welke lagere uitgaven gerealiseerd worden als gevolg van de vertraging van de invoer van het vernieuwde C2000. De voornoemde leden vragen of u dit kunt expliciteren voor de jaren 2017, 2018 en 2019 waarbij inzichtelijk wordt gemaakt welke kostensoorten het betreft en welke bedragen daaraan gekoppeld zijn.

5. Toekomstig mobiel breedband voor de Openbare Orde en Veiligheid-diensten (OOV-diensten)

De leden van de CDA-fractie vragen of u de stelling deelt dat het vernieuwde C2000 journalisten nagenoeg onmogelijk maakt om kennis te nemen van actuele activiteiten van hulpdiensten, de politie in het

bijzonder? Deelt u de mening dat hiermee de mogelijkheden van journalisten om verslag te doen tot een minimum worden teruggebracht? Deze leden vragen of u kan aangeven op welke wijze de persvrijheid – met name die voor fotojournalisten – vanuit de politie gefaciliteerd wordt? Bent u bereid een verkennende studie te laten verrichten over hoe in andere landen omgegaan wordt met de informatievoorziening rond actuele gebeurtenissen, vanuit de hulpverleningsdiensten wiens dataverkeer volledig gedigitaliseerd is? Deze leden vragen of u het standpunt deelt dat vrije nieuwsgaring ook bij digitaal dataverkeer tussen hulpverleners tot de mogelijkheden moet blijven behoren?

De leden van de D66-fractie lezen dat momenteel wordt bezien op welke wijze invulling gegeven kan worden aan de toekomstige behoefte aan mobiel breedband voor communicatie in de OOV-sector. Zij constateren dat dergelijk mobiel breedband in eerste instantie naast C2000 zal bestaan, om vervolgens de primaire communicatievorm te worden voor de sector. De aan het woord zijnde leden begrijpen hieruit dat hoewel het vernieuwde C2000 het huidige C2000-systeem nog niet heeft vervangen, er al wel vooruitgelopen wordt op weer een nieuw systeem. Is dit een juiste analyse? Waarom acht u het noodzakelijk en proportioneel om ondanks het feit dat het nieuwe C2000-systeem nog niet is ingevoerd, al wel een traject in gang wordt gezet naar een systeem waarin mobiel breedband de primaire communicatievorm wordt? Is het in dit geval niet mogelijk en logischer om vanaf het huidige C2000 systeem direct over te stappen naar een dergelijk nieuw communicatiesysteem? Welke kosten zijn gemoeid met het voorgestelde onderzoek naar het gebruik van mobiele breedband voor missiekritische communicatie?

6. Nieuwe meldkamers

De leden van de D66-fractie lezen dat in de huidige planning medio mei 2018 de nieuwe meldkamer in Rotterdam als eerste samengevoegde meldkamer worden aangesloten op de landelijke ICT-voorziening voor het meldkamerdomein. De aan het woord zijnde leden zijn benieuwd of dit inmiddels inderdaad het geval is? Zo nee, op welke termijn zal dit wel het geval zijn? Hoeveel vertraging heeft het in gebruik nemen van de meldkamer in Rotterdam in totaal opgelopen? Is het nog steeds de planning dat de meldkamers in Den Bosch en Haarlem volgend jaar volgen? Hoeveel vertraging heeft het in gebruik nemen van deze meldkamers in totaal opgelopen?

De leden van de SP-fractie vragen een reflectie op het proces van het samenvoegen van de meldkamers, nu niet in 2020 maar in 2021 het doel wordt gehaald. Deelt u de mening dat een reorganisatie van dit formaat niet samen gaat met een bezuiniging van deze omvang? Zo nee, wat is volgens u dan de reden dat dit proces zoveel moeilijkheden kent?

7. Stand van zaken 112

De leden van de SP-fractie vragen of er nu gegarandeerd kan worden dat ook in gebieden waar slecht mobiel bereik is, de bereikbaarheid van 112 wel gewaarborgd is.

II. Reactie van de Minister van Justitie en Veiligheid

1. Inleiding

Op 6 april jl. zond ik uw Kamer mijn brief Voortgang C2000, meldkamers en 112¹. Op 16 mei jl. vond een uitzending van het programma Zembla plaats over C2000. De vragen die u mij naar aanleiding van deze uitzending heeft gesteld beantwoord ik in deze brief. Voor de volledigheid zend ik hierbij tevens als bijlage de antwoorden die ik aan Zembla heb verstrekt op meerdere sets vragen die door hen in de voorbereiding van de uitzending zijn gesteld². Ook de reactie die mijn ministerie heeft gepubliceerd als reactie op de Zembla uitzending is bijgevoegd³.

De vernieuwing van een vitaal systeem als C2000 is een meerjarig en complex traject. Mijn ambtsvoorgangers en ik hebben uw Kamer daar de afgelopen jaren periodiek schriftelijk en mondeling over geïnformeerd. In onderstaande antwoorden komt een groot deel van deze informatie samen. Tevens is daarbij de aanvullende informatie die u mij heeft verzocht ten behoeve van de technische briefing van 21 november 2017⁴ behulpzaam.

Zoals in mijn eerdere brief opgenomen, bied ik uw Kamer graag aan om in een volgende technische briefing e.e.a. mondeling nader te laten toelichten.

2. Vernieuwing C2000 systeem

Aanbesteding

Voor een meer uitgebreide beschrijving van het aanbestedingstraject verwijs ik u naar de bijlage van Kamerstuk 25 124, nr. 87. Het huidige C2000 netwerk nadert het einde van de technologische levensduur. In 2014 is daarom gestart met de voorbereidingen van de aanbesteding⁵ voor vernieuwing van het netwerk. Voorafgaand, tijdens en na de aanbesteding zijn de aanbevelingen van de commissie Elias gevolgd en is gebruik gemaakt van de lessen uit de initiële implementatie van het huidige C2000-communicatienetwerk. Zo zijn de gebruikers (politie, defensie, brandweer en ambulancezorg) vanaf het begin op verschillende manieren betrokken geweest. Er is een marktverkenning uitgevoerd en voor het opstellen van het programma van eisen is gebruik gemaakt van kennis en expertise van de gebruikers en technisch specialisten van de beheerder (het Meldkamer Dienstencentrum van de politie) van het systeem. Bij de aanbesteding is een functionele uitvraag gedaan, dat wil zeggen dat de opdrachtgever het «wat» heeft uitgevraagd en dat de leveranciers invulling geven aan de «hoe»-vraag. Dit principe is in lijn met de aanbevelingen van de commissie Elias om maximaal gebruik te maken van de expertise van marktpartijen. Op 5 maart 2015 vond de voorlopige gunning plaats⁶ aan respectievelijk Hytera Mobilfunk GmbH (radionetwerk T2000), 2WAY B.V. (alarmeringsnetwerk P2000) en Eurofunk Kappacher GmbH (radiobediensysteem). Binnen de gestelde termijn heeft de enige andere aanbieder, tevens leverancier van het huidige systeem, bezwaar aangetekend tegen de

¹ Kamerstuk 25 124, nr. 89.

² Raadpleegbaar via www.tweedekamer.nl

³ Raadpleegbaar via www.tweedekamer.nl

⁴ Kamerstuk 25 124, nr. 87, bijlage

⁵ Kamerstuk 29 628, nr. 475.

⁶ Kamerstuk 25 124, nr. 74.

voorlopige gunningsuitslag van de aanbesteding⁷. Zowel in kort geding⁸ als in hoger beroep⁹ is het Ministerie van Justitie en Veiligheid in het gelijk gesteld. Hierna was in oktober 2015 de gunning definitief en ging het programma IVC (Implementatie Vernieuwing C2000) van start¹⁰.

De leden van de D66-fractie vragen of het klopt dat bij de aanbesteding is gekozen voor de meest goedkope optie. De leden van de D66 fractie verzoeken verder om de andere kandidaten en de bijbehorende offertes voor de aanbesteding van het nieuwe C2000 systeem aan de Kamer te doen toekomen.

De aanbestedingsfase Vernieuwing C2000 is gestart met een selectiefase, waarbij de partijen zijn geselecteerd op basis van eisen aan ervaring en referenties. De gunning heeft hierna plaatsgevonden op basis van het gunningscriterium van Economisch Meest Voordelige Inschrijving (EMVI), wat inhoudt dat zowel de kwaliteit als de prijs meewegen (dat wil zeggen: niet de prijs als zodanig, maar de prijs-kwaliteitverhouding). Uitgangspunt hierbij is dat een minimum kwaliteitsniveau is afgedongen door middel van «knock out» criteria. Bij de beoordelingen heeft de kwaliteit zwaarder gewogen dan de prijs, conform het aanbestedingsdossier. Informatie over de inhoud van uitgebrachte offertes is commercieel vertrouwelijk en kan ik daarom niet openbaar maken.

Toelichting opgelopen vertraging en huidige planning

De leden van de D66-fractie vragen om een overzicht te bieden van de stappen die de afgelopen jaren zijn gezet in de vernieuwing van C2000 en vragen tevens of daarbij kan worden aangegeven op welke momenten – en met welke reden – vertraging is opgelopen.

Voor een volledig overzicht van het verloop van het traject van de vernieuwing verwijs ik uw Kamer naar de bijlage die ik heb gestuurd bij mijn brief ter voorbereiding op de technische briefing van 21 november 2017¹¹. Deze is tevens bijgevoegd¹². Ik zal hier ingaan op de vraag op welke momenten en waardoor vertraging is ontstaan.

Het vernieuwen van een systeem als C2000 zal in alle gevallen een complexe en niet risicoloze onderneming zijn. Het is nooit volledig te voorzien welke vraagstukken zich tijdens het meerjarig traject zullen voordoen die leiden tot voortschrijdend inzicht en noodzakelijke aanpassingen in het traject. Zo heeft ook het BIT de complexiteit van het traject bevestigd. Ik stel daarbij kwaliteit altijd voor tijd. De veiligheid van hulpverleners en burgers staat voorop. Omdat vele partijen en veel (schaarse) capaciteit noodzakelijk zijn, moet er strak gepland en gestuurd worden en moet vanaf een vroeg stadium al worden gewerkt met een geplande migratiedatum.

De eerste vertraging ontstond doordat bleek dat in de planning onvoldoende tijd was opgenomen voor het gedegen, onafhankelijk testen van het systeem. Daarnaast bleek dat er een grotere diversiteit was in het gebruik van de apparatuur in de meldkamers, dan bij de aanbesteding was verondersteld. Om de nieuwe apparatuur van het vernieuwde C2000 te kunnen gebruiken in alle huidige meldkamers en op de toekomstige standaard werkplek van de Landelijke Meldkamer Organisatie was extra tijd nodig. Als gevolg hiervan is meer tijd genomen in de planning voor

⁷ Kamerstuk 25 124, nr. 75.

⁸ Kamerstuk 25 124, nr. 76.

⁹ Kamerstuk 25 124, nr. 77.

¹⁰ Kamerstuk 25 124, nr. 78.

¹¹ Kamerstuk 25 124, nr. 87, bijlage

¹² Raadpleegbaar via www.tweedekamer.nl

het testen van het systeem en het aanpassen van dit onderdeel voor de meldkamerbediening.

In juli 2017 heb ik uw Kamer geïnformeerd¹³ dat was besloten de geplande migratiedatum in november 2017 los te laten en tot een nieuwe planning te komen. Deze tweede vertraging ontstond omdat de leveranciers aangaven het vernieuwde C2000 niet op tijd te kunnen opleveren. Vooral de *integratie* van de drie delen van het systeem bleek hierin de oorzaak van de vertraging.

Bij het uitwerken van een aangepaste planning bleek dat een geïntegreerde oplevering van het systeem in 2018 weliswaar mogelijk was, maar dat daarbij nog aanzienlijke onzekerheden aanwezig waren. Om deze onzekerheden te beperken, met als uitgangspunt om voor de minst risicovolle migratiestrategie te kiezen, is er in dit stadium voor gekozen om de vernieuwingen van T2000 (spraak), P2000 (berichten) en de radiobediening in de meldkamers van elkaar los te koppelen. Begin februari 2018 heb ik uw Kamer vervolgens geïnformeerd¹⁴ over de nieuwe, gefaseerde planning.

Ik heb in juni 2018 Bureau Gateway Review opdracht gegeven een audit uit te voeren om te bezien of de door het programma IVC gekozen aanpak in het nieuwe migratiescenario voldoende zeker stelt dat de migratie naar het nieuwe T2000-spraaknetwerk in 2018 wordt gerealiseerd. Het reviewteam constateert een brede steun voor de gekozen aanpak van het programma IVC. «De logische stappen worden gezet. Nieuwe ontwikkelingen worden getest door een onafhankelijke partij, er worden kwaliteitsaudits gedaan en er wordt gestuurd op de integraliteit van het op te leveren resultaat. Daarnaast wordt veel aandacht besteed aan bij een migratie mogelijk optredende scenario's en aan technische mitigerende maatregelen. Het programma besteedt de nodige aandacht aan het complexe speelveld van belanghebbende partijen met verschillende eigenaren en sturingsrelaties.»

Het reviewteam is van mening dat de gekozen programma aanpak een succesvolle migratie optimaal faciliteert. Het reviewteam doet een aantal aanbevelingen die inmiddels van opvolging worden voorzien door het programma IVC. Ik voeg het Gateway rapport als bijlage bij deze brief¹⁵.

De leden van de CDA-fractie vragen wat thans de exacte implementatiedata zijn per regio/meldkamer en vragen mij dit te specificeren voor zowel de implementatie van het nieuwe spraaknetwerk (koppeling aan de huidige radiobediening in de meldkamers) als voor de (in 2019 voorziene) koppeling van de nieuwe radiobediening aan het vernieuwde spraaknetwerk.

Begin februari 2018 heb ik uw Kamer geïnformeerd¹⁶ over de nieuwe, gefaseerde planning. Deze fasering betreft de verschillende technische onderdelen van het systeem (respectievelijk alarmering, spraak en radiobediening). Per onderdeel gaat de vernieuwing landelijk in één keer, dus niet gefaseerd per regio of meldkamer. De vernieuwing van het alarmeringsnetwerk (P2000) heeft inmiddels plaatsgevonden conform planning, begin juni 2018. De vernieuwing van het spraaknetwerk (T2000) is gepland voor najaar 2018 (koppeling aan de huidige radiobediening). De vernieuwing van de radiobediening in alle meldkamers (koppeling aan het vernieuwde T2000) is gepland voor 2019.

¹³ Kamerstuk 25 124, nr. 86.

¹⁴ Kamerstuk 25 124, nr. 88.

¹⁵ Raadpleegbaar via www.tweedekamer.nl

¹⁶ Kamerstuk 25 124, nr. 88.

De leden van de CDA-fractie vragen of ik nog steeds van mening ben dat de drie bij de vernieuwing van C2000 betrokken marktpartijen in staat zijn om het door hen aangenomen werk daadwerkelijk binnen een redelijke termijn uit te voeren.

Ik heb naar aanleiding van de tweede ontstane vertraging een externe audit laten uitvoeren bij Hytera en Eurofunk op de technische aspecten van het nieuwe systeem, zoals de architectuur en de kwaliteit van de software van het vernieuwde C2000 systeem¹⁷. De auditinstantie (Xebia) oordeelt dat er geen significante bevindingen in de architectuur van de leveranciers zijn die een succesvolle migratie in de weg staan. De vernieuwingspartners hebben sinds de overgang naar de gefaseerde migratiestrategie hun organisatie met hulp van de programmaorganisatie verder versterkt met extra mensen en extra expertise.

De vernieuwing van een groot en complex systeem als C2000 is een ingrijpend traject. Ook met de contractpartners van het huidige netwerk zou een vernieuwing van deze omvang en complexiteit risico's met zich meebrengen. Volledige zekerheden in de planning zijn daarbij nooit te krijgen.

De leden van de CDA-fractie vragen of ik hierbij specifiek kan ingaan op de verwachtingen ten aanzien van Hytera Mobilfunk GmbH, mede gelet op hetgeen in de Zembla-uitzending ten aanzien van deze firma naar voren is gebracht.

Ik hecht eraan de integrale verantwoordelijkheid van de drie leveranciers in stand te houden en niet op te splitsen. De combinatie van de drie leveranciers is verantwoordelijk voor de oplevering van het complete systeem.

Chinese aandeelhouder van Hytera Mobilfunk GmbH

De leden van de CDA-fractie en D66-fractie vragen of het klopt dat Hytera Mobilfunk GmbH een Duitse dochteronderneming is van het Chinese bedrijf Hytera Communications, dat goede zakelijke betrekkingen onderhoudt met de Chinese overheidsdiensten.

De leverancier van het vernieuwde mobiele spraaknetwerk T2000 is het Duitse bedrijf Hytera Mobilfunk GmbH (hierna: HMF). HMF is een van oorsprong Duits bedrijf (Rohde und Schwarz), dat in 2012 is overgenomen door de Chinese maatschappij Hytera Communications Ltd.

De leden van de D66-fractie vragen of Hytera ten tijde van de aanbesteding al in Chinese handen was en zo ja, of dit bij het toekennen van de opdracht meespeelde. En zo nee, of ik het verantwoord acht om een voor de Nederlandse veiligheid essentieel missiekritisch netwerk aan een Chinese partij te gunnen en of het ministerie, mocht het op dat moment hebben geweten dat Hytera in Chinese handen zou komen, de opdracht ook zou hebben gegund of mogelijk aanvullende voorwaarden zou hebben gesteld. De leden van de PvdA-fractie vragen wat er nu nog gedaan kan worden om te voorkomen dat dit deel van de vitale infrastructuur van C2000 door sabotage vanuit China wordt bedreigd.

Het Duitse HMF heeft zelfstandig ingeschreven op de aanbesteding. Het feit dat het een dochteronderneming is van een Chinese aandeelhouder was op dat moment bekend en is destijds ook aan uw Kamer gemeld¹⁸. Dit is geen belemmering geweest voor de gunning. C2000 wordt gebruikt voor de reguliere communicatie tussen de hulpverleningsdiensten: politie, brandweer, ambulance en Koninklijke Marechaussee. Het beveiligings-

¹⁷ Ter vertrouwelijke inzage tot aan het herfstreces 2018: Xebia Architecture Inspection C2000 d.d. sept 2017 (audits Eurofunk en Hytera). Ter vertrouwelijke inzage gelegd, alleen voor de leden, bij het Centraal Informatiepunt Tweede Kamer

¹⁸ Kamerstuk 25 124, nr. 77.

niveau voor deze gebruikersgroepen is bepaald op het niveau «departementaal vertrouwelijk». Ook het beveiligingsniveau van het vernieuwde netwerk zal als zodanig worden ingericht. De communicatie via het C2000-netwerk is versleuteld en maakt gebruik van afgeschermd verbindingen. Gebruikers kunnen extra versleuteling toepassen indien nodig. Er zijn bij het classificatieniveau passende maatregelen genomen om sabotage te herkennen en te voorkomen. Voor een uitgebreide toelichting op de beveiliging van radiocommunicatie via de TETRA-standaard in relatie tot het beveiligingsniveau van C2000, waarin aandacht voor beschikbaarheid, integriteit en vertrouwelijkheid, verwijs ik uw Kamer naar de brief van 18 april 2016¹⁹. Daarin heeft mijn ambtsvoorganger uw Kamer met betrekking tot de mogelijkheid van interceptie via een zogenaamde «verborgen achterdeur» gemeld dat zowel politie als AIVD hebben aangegeven vanuit haar informatielijn nooit een «achterdeur» te hebben aangetroffen of aanwijzingen dat hiervan gebruik wordt gemaakt vernomen. Zowel politie als AIVD gaven verder aan dat het moedwillig in de apparatuur zaken inbouwen om de communicatiesystemen te kunnen af luisteren, hoewel theoretisch niet uit te sluiten, vooralsnog niet gestaafd is door bewijs of concrete vermoedens.

Positie inlichtingen- en veiligheidsdiensten

Zoals mijn ambtsvoorganger uw Kamer heeft gemeld in de beginfase van de vernieuwing van C2000²⁰, is met het Nationaal Bureau Verbindingsbeveiliging (NBV) van de AIVD afgesproken dat zij tijdens de implementatie van het systeem een adviserende rol vervullen in de realisatie van het beveiligingsniveau «departementaal vertrouwelijk». Gedurende het traject van de vernieuwing ben ik dan ook in contact met het NBV hierover. Zo heb ik het NBV eind 2017 om advies gevraagd voor het laten uitvoeren (later dit jaar) van een penetratietest op het nieuwe systeem.

Uiteraard houd ik de veiligheid van de systemen die gebruikt worden goed in de gaten en heeft het kabinet aandacht voor ontwikkelingen in technologieën en kwetsbaarheden daarin, en de noodzaak scherp te blijven op de beveiliging hiervan. Ook de internationale ontwikkelingen rond Chinese partijen worden door mijn departement gevolgd.

De leden van de CDA-fractie en de PvdA-fractie vragen of het klopt dat de AIVD/MIVD ernstige bezwaren/zorgen hebben inzake de betrokkenheid van een Chinese partij bij de bouw van C2000, zoals gesteld werd in de voornoemde uitzending van Zembla. De leden van de PvdA-fractie vragen of deze zorgen bij mij reeds bekend waren en zo ja, vanaf welke datum, en vragen wat ik naar aanleiding van deze waarschuwing heb gedaan. De stelling dat de AIVD en/of MIVD ernstige bezwaren zouden hebben tegen de betrokkenheid van een Chinese partij bij de vernieuwing van C2000 en/of dat het systeem tegen de zin van de AIVD zou zijn aangekocht, is onjuist.²¹

De leden van de CDA-fractie vragen of ik, mede in het licht van regeringsopstelling ten opzichte van Kaspersky, kan uitleggen hoe ik nu tegen deze situatie aankijk en of het nodig is dat aanvullende maatregelen worden genomen om risico's in te perken. De leden van de VVD-fractie vragen mij in dit verband aan te geven waarom Nederland met een Russisch antivirussoftware-bedrijf geen zaken kan doen, maar het communicatie-

¹⁹ Kamerstuk 29 628, nr. 631.

²⁰ Kamerstuk 25 124, nr. 74.

²¹ Zie de antwoorden die ik aan Zembla heb verstrekt in antwoord op meerdere sets vragen die door hen in de voorbereiding van de uitzending zijn gesteld, Raadpleegbaar via www.tweede-kamer.nl.

netwerk van onze hulp- en veiligheidsdiensten wel door een Chinees bedrijf (Hytera) ingericht kan worden. De leden van de D66-fractie vragen hoe het gunnen van de opdracht aan Hytera zich verhoudt tot uitspraken van de AIVD-directeur eerder dit jaar, waarin hij stelt dat China tot één van de drie grootste bedreigingen voor de cyberveiligheid behoort, aangedreven door de overheid. De leden van de PvdA-fractie vragen of ik de mening van de directeur van de AIVD deel dat er in zijn algemeenheid vanuit China sprake is van cyberdreiging en zo ja, of ik de dreiging van sabotage van C2000 door China een reële dreiging acht, en zo nee, waarom niet.

De voorzorgsmaatregel die door het kabinet is genomen²² gaat over een specifiek product, namelijk antivirussoftware van Kaspersky. Het kabinet beziet de risico's die verbonden kunnen zijn aan digitale producten en diensten op een zorgvuldige «case by case» basis en eventuele maatregelen worden individueel afgewogen. Gezien de nationale veiligheidsbelangen en de belangen van het bedrijfsleven wordt niet vooruitgelopen op gespeculeerd over al dan niet mogelijke toekomstige maatregelen. In het geval van Kaspersky antivirussoftware is het een combinatie van factoren die ertoe heeft geleid dat sprake is van risico's voor de nationale veiligheid die het kabinet wil mitigeren. Antivirussoftware zit diep in de systemen en kan bij misbruik leiden tot een groot veiligheidsrisico. Russische wetgeving verplicht bedrijven als Kaspersky samen te werken met de Russische overheid en Rusland heeft daarnaast een actief offensief cyberprogramma dat onder meer gericht is op Nederland en Nederlandse belangen.

Op het moment dat de veiligheidsdiensten aanleiding zien voor risico's voor het C2000 netwerk, zal ik daarvoor passende maatregelen treffen.

De leden van de D66-fractie vragen waarop ik de stelling baseer dat C2000 een voor hackers «onneembare vesting» is, zoals gesteld in de voornoemde Zembla-uitzending.

Ik herken mij niet in deze stelling. Zoals ik eerder in deze beantwoording al deed, verwijs ik uw Kamer voor een uitgebreide toelichting op de beveiliging van radiocommunicatie via de TETRA-standaard naar mijn brief van 18 april 2016²³.

Dekking C2000

De leden van de D66-fractie vragen hoeveel dekkingsissues momenteel nog open staan en op welke wijze wordt bepaald dat dekkingsissues op bepaalde plekken lage prioriteit genieten.

Het huidige C2000 heeft op dit moment een radiodekking van 97,8%. Nederland behoort daarmee in Europa tot de landen met de beste dekking. Als gevolg van veranderingen in bebouwing en landschap zullen er altijd locaties ontstaan (en soms verdwijnen) waar de dekking niet optimaal is.

Het ontstaan en oplossen van dekkingsissues is dan ook een permanent proces. Hiervoor bestaat een landelijke, objectieve systematiek om te prioriteren welke issues als eerste worden aangepakt, de zogeheten DIPP (Dekkings Issues Prioriterings Procedure). Met deze werkwijze wordt door alle kolommen gezamenlijk en op landelijk niveau, de prioritering vastgesteld op basis van incidentregistraties en risicoanalyse. De DIPP-lijst is niet statisch, maar wordt periodiek geactualiseerd. Daarbij worden eventueel nieuwe issues opgenomen en bestaande issues opnieuw op urgentie gewogen, in samenspraak met de hulpverleningsdiensten. Het is dus nadrukkelijk geen chronologische «wachlijst» waarbij een issue na

²² Kamerstuk 30 821, nr. 46

²³ Kamerstuk 29 628, nr. 631.

verloop van tijd vanzelf bovenaan staat. Voor een dekkingsissue met een lage prioriteit kan het ook voorkomen dat er meerdere jaren achtereen steeds andere issues meer urgentie krijgen en het dus langer duurt voordat deze worden opgelost. Die lage prioriteit is dan wel vastgesteld op basis van een objectieve procedure en gezamenlijke besluitvorming. Momenteel staan er 34 dekkingsissues open.

De leden van de D66-fractie vragen wat de gemiddelde looptijd is waarin dekkingsissues opgelost worden en hoe deze looptijd bij een dekkingsissue met hoge versus lage prioriteit varieert.

De tijd dat een issue op de DIPP-lijst staat, kan zoals hierboven toegelicht sterk variëren. Vanaf het moment dat een issue wordt aangemerkt om op te lossen, wordt de doorlooptijd daarvoor bepaald door meerdere factoren. De meeste tijd kost het verwerven van een locatie (perceel) waar een opstelpunt kan worden geplaatst. Ondanks het vergunningsvrij mogen bouwen, kan dit geruime tijd vergen (dit verschilt per locatie, door onder meer bewoners-consultatie, daadwerkelijke verwerving, Natura 2000 toets, beschermd stadsgezicht, etc.). Daarna volgen de daadwerkelijke bouw en realisatie, dit kan binnen enkele maanden gerealiseerd worden.

De leden van de D66 fractie-vragen hoe ik uitsluit dat in dergelijke gebieden grote calamiteiten plaatsvinden waarvoor toereikende dekking van C2000 wel degelijk noodzakelijk is.

Ik interpreteer de vraag van de leden van de D66-fractie in deze context als de vraag hoe ik kan uitsluiten dat zich een calamiteit voordoet in een gebied met een laag geprioriteerd dekkingsissue. Uiteraard valt een calamiteit op geen enkele locatie 100% uit te sluiten, maar ik wijs er nadrukkelijk op dat een risicoanalyse onderdeel uitmaakt van de DIPP-afweging. Een lage prioritering houdt dus in een lage inschatting van de kans op en/of impact van incidenten of calamiteiten op die locatie. Tot slot kunnen daar waar nodig en mogelijk tussentijdse tijdelijke oplossingen worden ingericht, zoals een mobiel of tijdelijk opstelpunt.

De leden van de D66-fractie en de CDA-fractie vragen of ik de meest recente versie van de DIPP-lijst aan de Kamer kan doen toekomen, dan wel vertrouwelijk ter inzage leggen, en of ik bereid ben updates van deze lijst periodiek aan de Kamer te doen toekomen, en zo nee, waarom niet. Het openbaar maken van een lijst met locaties waar mogelijk geen optimaal C2000-bereik voor de hulpdiensten is acht ik in strijd met het belang van de openbare orde en veiligheid. Ik zal de DIPP-lijst dan ook niet openbaar aan de Kamer doen toekomen, maar ben wel bereid deze vertrouwelijk ter inzage te leggen²⁴.

Maatregelen «Gouden Uur»

De leden van de respectievelijke fracties hebben naar aanleiding van de Zembla-uitzending zorgen geuit over de beschikbaarheid en capaciteit van het C2000 netwerk in een situatie van een grote calamiteit, zoals een terroristische aanslag. Er zijn vele, in detail uitgewerkte vragen gesteld. Ik geef uw Kamer allereerst een algemene, overkoepelende toelichting op de maatregelen die zijn getroffen rondom het zogeheten Gouden Uur (het eerste uur na een groot incident) en ga daarna in op de resterende vragen die daarmee nog niet zijn beantwoord.

²⁴ Ter vertrouwelijke inzage tot aan het herfstreces 2018: DIPP-lijst begin 2018, ter vertrouwelijke inzage gelegd, alleen voor de leden, bij het Centraal Informatiepunt Tweede Kamer.

Het C2000-netwerk is toegerust om de hulpdiensten te ondersteunen, ook bij calamiteiten. Eerder is met het Verbeterproject C2000²⁵ en het project Portogewoon²⁶ veel verbeterd. De zogeheten etherdiscipline en het juiste gebruik van de C2000 portofoons (onder meer naar aanleiding van de ervaringen bij de poldercrash in 2009) zijn daarin belangrijke aandachtspunten geweest. Voorts krijgt het vernieuwde C2000 de beschikking over een zogenaamde calamiteiten laag: een grotere capaciteit om onverwachte pieken in de belasting van het netwerk op te vangen. Er zal echter altijd een bovengrens aan de capaciteit van het systeem blijven bestaan. Deze wordt hoofdzakelijk bepaald door de schaars beschikbare radiofrequenties. Wanneer er bij grote, acuut optredende calamiteiten een plotselinge, onvoorziene, zeer grote capaciteitsvraag ontstaat zou het systeem overbelast kunnen raken. Ervaringen in het buitenland met terroristische aanslagen hebben dit aangetoond. Dit heeft zich bijvoorbeeld voorgedaan bij de aanslagen in Brussel in maart 2016²⁷.

Tijdens een zogeheten «Gouden Uur» is ongestoorde communicatie voor de hulpverleningsdiensten van vitaal belang. Juist daarom heeft het Ministerie van Justitie en Veiligheid eind 2016 de procedures voor het gebruik van C2000 aangescherpt. Het betreft hier additionele maatregelen die zien op zeer specifieke omstandigheden, waarvan het effect merkbaar kan zijn voor een specifiek afgebakend gebied. Deze maatregelen zijn multidisciplinair afgestemd en van technische en operationele aard. De maatregelen houden in dat de belangrijkste gesprekken op het netwerk voorrang hebben op minder belangrijke gesprekken. De primaire gebruikers van het systeem krijgen voorrang met een vastgesteld aantal gespreksgroepen per kolom: politie, brandweer, ambulancediensten en het Ministerie van Defensie. Deze prioriteitsstelling kan op basis van de situatie dynamisch worden uitgebreid naar andere functionarissen of organisaties. De meldkamer van het verzorgingsgebied waar de aanslag plaatsvindt, heeft de volledige regie op de communicatie, bepaalt het moment van op- en afschalen naar (vooraf vastgestelde) prioritaire gespreksgroepen en kan bijvoorbeeld oproepen tot radiostilte.

Naast de primaire gebruikers kent C2000 ook nog gelieerde gebruikers en bijzondere gebruikers²⁸. Standaard hebben de gespreksgroepen van de gelieerde en bijzondere gebruikers een lagere prioriteit in het netwerk dan de gespreksgroepen van de aangewezen gebruikers. Wanneer de meldkamer de vastgelegde Gouden-Uur-maatregelen in werking stelt, kan het gebeuren dat een gesprek op een niet geprioriteerde gespreksgroep mogelijk wordt afgebroken ofwel pas na enkele seconden tot stand komt omdat een geprioriteerde gespreksgroep voorrang krijgt. Het gaat hierbij om hun communicatie met de meldkamer en hulpdiensten; voor hun onderlinge communicatie maken zij dan waar nodig gebruik van hun eigen communicatiesystemen. Het Ministerie van Justitie en Veiligheid heeft hierover met de hulpverleningsdiensten afspraken gemaakt en de aangewezen gebruikers stemmen af met hun gelieerde gebruikers.

Met deze maatregelen en afspraken zijn zowel het systeem als de gebruikers ervan zo goed mogelijk voorbereid op een specifieke situatie zoals een terroristische aanslag.

²⁵ Kamerstuk 25 124, nr. 73.

²⁶ Kamerstuk 25 124, nr. 77.

²⁷ België kent evenals Nederland een TETRA netwerk voor de communicatie van de hulpdiensten.

²⁸ Zie Beleidsregels over de toelating en het gebruik van het radiocommunicatienetwerk C2000 door derden, 2 december 2009, Stcrt (2009), nr. 19742.

De leden van de PvdA-fractie vragen naar aanleiding van het gestelde in de Zembla-uitzending of er sprake is van een noodplan om het probleem van overbelasting van het systeem bij calamiteiten op te lossen en zo ja, wat dit inhoudt.

De Gouden-Uur maatregelen zijn het noodplan.

De leden van de D66-fractie vragen of ik het door Zembla geciteerde document aan de Kamer kan doen toekomen.

Het document waarnaar in de Zembla-uitzending wordt verwezen, betreft de brief van 23 december 2016 waarin de afspraken rondom het Gouden-Uur formeel worden bevestigd aan alle betrokken partijen²⁹. Ik voeg deze brief als bijlage bij deze brief³⁰. De maatregelen zijn o.a. verwerkt in het Handboek C2000 van het Instituut voor Fysieke Veiligheid³¹.

Door de Groen Links-fractie is, naar aanleiding van het gestelde in de Zembla uitzending, tijdens het Algemeen Overleg Nucleaire veiligheid d.d. 17 mei 2018 een vraag gesteld aan de Staatssecretaris van Infrastructuur en Waterstaat over de mogelijkheid om zwaardere, grotere zendmasten te plaatsen in de grensregio met het oog op mogelijke calamiteiten bij de kerncentrales Borssele en Doel (Kamerstuk 25 422, nr. 224). De leden van de PvdA-fractie vragen of het waar is dat bijvoorbeeld voor de kerncentrale in Borssele, huisartsenposten of reddingsbrigades de kans bestaat dat communicatie via C2000 niet meer mogelijk is en welke risico's dit met zich mee brengt. De Staatssecretaris van Infrastructuur en Milieu heeft mij gevraagd deze vraag over C2000 te beantwoorden en dat doe ik graag in samenhang met het bovenstaande.

Zoals hierboven toegelicht houden de Gouden-Uur maatregelen in dat de primaire gebruikers van het C2000 systeem voorrang krijgen (politie, brandweer, ambulancediensten en het Ministerie van Defensie). De gespreksgroepen van de gelieerde gebruikers (bijvoorbeeld een kerncentrale) en bijzondere gebruikers hebben standaard een lagere prioriteit in het netwerk dan de gespreksgroepen van de aangewezen gebruikers. Deze prioriteitsstelling kan echter op basis van de situatie worden uitgebreid naar andere functionarissen of organisaties. De meldkamer van het verzorgingsgebied waar het incident plaatsvindt, heeft hierop de volledige regie.

Ter informatie meld ik uw Kamer dat bijvoorbeeld de eigenaar van kerncentrale Borssele (Elektriciteits Productie-maatschappij Zuid-Nederland), mij heeft laten weten dat C2000 voor hen geen eerste-lijns communicatiemiddel is en dat zij ervan op de hoogte zijn dat de regie van het gebruik van C2000 door anderen bepaald kan worden in geval van een calamiteit. EPC maakt tijdens een calamiteit of crisis gebruik van andere middelen. EPZ heeft dit voorafgaand aan de uitzending ook aan Zembla laten weten.

3. Continuïteit huidige C2000 netwerk

Stabiliteit en storingsgevoeligheid

De leden van de PvdA-fractie vragen, evenals de leden van de D66-fractie en de CDA-fractie, op basis van welk extern onderzoek blijkt dat het huidige C2000 systeem zich nog robuust en stabiel gedraagt. Voornoemde

²⁹ te weten de Secretaris-generaal van het Ministerie van Defensie, de portefeuillehouder Informatievoorziening Veiligheidsberaad, de Korpschef van Politie en de Voorzitter van Ambulancezorg Nederland.

³⁰ Raadpleegbaar via www.tweedekamer.nl

³¹ Zie <https://www.ifv.nl/kennisplein/Documents/201712-BrwNL-Handboek-C2000.pdf>

leden vragen uit welk onderzoek dit is gebleken, of ik dit onderzoek aan de Kamer kan doen toekomen, dan wel vertrouwelijk ter inzage kan leggen en zo nee, waarom niet.

Ik heb naar aanleiding van het uitstel van de migratie in 2017 zowel door de beheerder van het C2000 netwerk (MDC) als door de externe partij Xebia onderzoek laten doen naar het huidige systeem.

- Uit het MDC-onderzoek is gebleken dat het huidige systeem stabiel is en geen significant hoger aantal storingen laat zien dan in de afgelopen jaren. De conclusie luidt: «Op basis van de feitelijke verstoringen van de afgelopen twee jaar en de storingsanalyse is het netwerk stabiel en de continuïteit geen reden tot zorg».
- De hoofdconclusie van het Xebia onderzoek luidt als volgt: «Uit de incidentenregistratie blijkt niet dat er sprake is van een exponentiële stijging van het aantal incidenten.» De huidige C2000-oplossing kent sinds 2008 een redelijk stabiele stroom van incidenten en reparaties waardoor hogere faalkansen worden voorkomen. Dit is een normaal beeld voor een systeem van deze omvang en complexiteit dat zich in de levensfase van het huidige C2000 bevindt. In deze levensfase behoeft het systeem voortdurend onderhoud, waarmee wordt voorkomen dat het terechtkomt in een fase waarin sprake is van een exponentiële toename in het aantal incidenten. Vanwege de technisch of commercieel vertrouwelijke informatie kan ik het volledig rapport niet openbaar maken, maar ik ben bereid dit vertrouwelijk ter inzage te leggen³². Tijdens een eventuele technische briefing kan hierop een nadere toelichting worden gegeven indien gewenst.

Gebaseerd op de conclusies uit de onderzoeken van MDC en Xebia concludeer ik dat het huidige systeem zich robuust en stabiel gedraagt.

De leden van de CDA-fractie vragen of ik de in het programma Zembla naar voren gebrachte stelling onderschrijf dat het huidige C2000 steeds storingsgevoeliger wordt. De leden van de D66-fractie vragen of het klopt het dat het huidige C2000 systeem steeds meer storingen ondervindt.

Zoals hierboven toegelicht blijkt uit intern en extern onderzoek dat geen sprake is van een exponentiële stijging van het aantal storingen. Dat wil uiteraard niet zeggen dat er geen storingen zijn; elk grootschalig ICT-systeem heeft te maken met storingen. Van veel van de verstoringen merkt de gebruiker niets, omdat deze niet leiden tot functieverlies. Dit kan zijn van een defect slot op een opstelpunt tot een defecte bedienpositie in een meldkamer. In de registratie worden *alle* soorten verstoringen opgenomen en wordt er door de beheerorganisatie vervolgens actie op genomen.

De leden van de VVD-fractie vragen of het in de Zembla uitzending op basis van een interne memo van de politie genoemde aantal van 2.775 storingen tussen april 2015 en augustus 2017 klopt.

De uitkomsten van het voornoemde MDC-onderzoek zijn weergegeven in een memo aan de Stuurgroep IVC. Dit memo is eerder in het kader van een WOB-verzoek openbaar gemaakt³³ en het is dit memo waaraan in de Zembla-uitzending werd gerefereerd. Dit document bevat het genoemde aantal van 2.775 storingen tussen april 2015 en augustus 2017. Overigens had het grootste deel van deze storingen geen invloed op de dienstverlening en konden de meeste storingen binnen de daarvoor afgesproken normtijden opgelost worden.

³² Ter vertrouwelijke inzage tot aan het herfstreces 2018: Xebia Second Opinion Continuïteit in 2019 d.d. jan 2018, ter vertrouwelijke inzage gelegd, alleen voor de leden, bij het Centraal Informatiepunt Tweede Kamer

³³ Link naar totale WOB-document (MDC-memo te vinden op p. 163, 164): zie <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/wob-verzoeken/2018/02/22/besluit-wob-verzoek-over-implementatie-van-vernieuwd-c2000-netwerk/Bijlagen.pdf>

De leden van de VVD-fractie vragen hoe ik een dergelijk aantal storingen kan rijmen met een robuust systeem en bij hoeveel storingen ik C2000 niet meer robuust vind. De leden van de D66-fractie vragen of het klopt dat het huidige C2000 systeem steeds meer storingen ondervindt en zo ja, hoe dit zich verhoudt tot de stellingname dat het huidige C2000-systeem zich de afgelopen jaren heeft ontwikkeld tot een «systeem dat zich robuust en stabiel gedraagt».

De robuustheid van het systeem is niet te definiëren in absolute (maximum) aantallen storingen, maar dient te worden gezien vanuit de meerjarige ontwikkeling en trends. Deze laat een robuuste lijn zien.

De leden van de ChristenUnie-fractie vragen hoe robuust de dekkingsgraad van het systeem is, vanaf welk moment er volgens mij sprake was van een robuust systeem en welke lessen er zijn geleerd van de ontwikkeling van het huidige systeem. De leden van de D66-fractie vragen of ik een overzicht kan geven van het aantal storingen met het huidige C2000 systeem in de afgelopen vijf jaar, uitgesplitst per maand.

C2000 kent al jarenlang een zeer hoge beschikbaarheid. De beschikbaarheid is één van de kritische prestatie-indicatoren van het C2000-beheer, met als norm 98%. De afgelopen jaren is de beschikbaarheid steeds ruim boven deze norm geweest, over de afgelopen vijf jaar (2013–2017) gemiddeld 99,84%³⁴.

Gebruik van alternatieven voor C2000

De leden van de D66-fractie vragen of het klopt dat sommige recherche-teams van de politie alternatieve communicatiemiddelen aanschaffen omdat het vertrouwen in het C2000 systeem te ver is afgenomen, zoals is gesteld in de voornoemde Zembla-uitzending en zo ja, hoe dit zich verhoudt tot de stellingname dat het huidige C2000 systeem zich de afgelopen jaren heeft «ontwikkeld tot een robuust systeem waar de hulpverleningsdiensten op kunnen vertrouwen».

Mijn ambtsvoorganger heeft uw Kamer in 2016 gemeld³⁵ dat de politie in haar werkwijze rekening houdt met het gebruik van detectieapparatuur zoals Target Blu Eye door derden. Dit kan betekenen dat in specifieke situaties geen gebruik wordt gemaakt van C2000, maar van alternatieve middelen. Hulpdiensten dienen in het kader van bedrijfscontinuïteit altijd rekening te houden met een mogelijke uitval van systemen, waaronder C2000, en dienen zij te beschikken over alternatieve communicatiemogelijkheden of procedures die tijdelijk inzetbaar zijn. Overigens bevat de Zembla uitzending voor een deel interviews uit het jaar 2009. Inmiddels zijn de verbetertrajecten C2000 en het project Portogewoon afgerond.

Maatregelen continuïteit 2019

De leden van de CDA-fractie vragen met welke firma's een contract is gesloten om het functioneren van het huidige C2000 – in brede zin – na 2018 te kunnen continueren.

Voor het eventuele onderhoud voor het bestaande C2000 netwerk in 2019 is Nokia gecontracteerd. Nokia werkt hierin samen met Koning en Hartman, een partij die al vanaf de start van C2000 op verschillende wijzen betrokken is bij het huidige systeem en ook het onderhoud op het nieuwe systeem zal gaan uitvoeren. Voor het onderhoud van het huidige radiobediensysteem na 2018 is de bouwer van het systeem, Kolibri Systems BV, gecontracteerd.

³⁴ Bron: meerjarenoverzicht kpi's, uit jaarverslag 2017 (wordt binnenkort gepubliceerd via www.c2000.nl)

³⁵ Kamerstuk 25 124, nr. 79
Kamerstuk 29 628, nr. 631

De leden van de PvdA-fractie vragen of het waar is dat het onderhoudscontract tot eind 2019 loopt en of er dan sprake is van een volledig operationeel nieuw systeem. Genoemde leden vragen tot wanneer het bestaande C2000 in technische zin volledig operationeel kan blijven. De vervanging van het spraaknetwerk is in de huidige planning voorzien voor najaar 2018. Het contract met Nokia is gesloten voor heel 2019.

De leden van de VVD-fractie vragen of ik op basis van de gemaakte contractuele afspraken kan garanderen dat het huidige C2000, indien dat in 2019 nog gebruikt moet worden, accuraat blijft functioneren, ook in geval van zwaar gebruik, zoals bijvoorbeeld het geval kan zijn na een terroristische aanslag.

Het huidige C2000-netwerk is en blijft, indien noodzakelijk, toegerust om de hulpdiensten in 2019 te ondersteunen, ook bij calamiteiten. Overigens merk ik op dat volledig risicoloze alternatieven niet bestaan. Niet voor het huidige C2000 netwerk, niet voor het nieuwe C2000 netwerk en niet voor het traject van de vernieuwing. Juist daarom kiest het Ministerie van Justitie en Veiligheid steeds voor de minst risicovolle alternatieven, voorzien van passende maatregelen en zo nodig onderbouwd door externe adviezen.

Onderdelen en updates

De leden van de CDA-fractie en de VVD-fractie vragen of ik de in het programma Zembla naar voren gebrachte stelling onderschrijf dat vervangingsonderdelen – ook voor bijvoorbeeld portofoons – moeilijk of niet meer te verkrijgen zijn. De leden van de VVD- vragen voorts of het klopt dat reserve-onderdelen niet meer gemaakt of geleverd worden nu Motorola de ontwikkeling en het onderhoud van C2000 heeft gestaakt, of ik kan aangeven hoe een leverancier een reserve-onderdeel kan aanleveren dat niet meer gemaakt wordt en of ik de mening deel dat het een veiligheidsrisico met zich meebrengt wanneer gewerkt wordt met verouderd materiaal waarvoor geen reserve-onderdelen meer beschikbaar zijn.

Ten aanzien van het onderhoud van de hardware zijn vergelijkbare afspraken met Nokia gemaakt als met de huidige leverancier. Nokia heeft ons laten weten op schema te liggen met het verwerven van de reserve-onderdelen. Nokia heeft contracten gesloten met een aantal toeleveranciers voor de verwerving van reserve-onderdelen. Het gaat daarbij deels om generieke (niet door of namens Motorola geproduceerde onderdelen) en deels om specifieke onderdelen (door of namens Motorola geproduceerde onderdelen). Verder maakt Nokia gebruik van de basisvoorraad onderdelen van het Ministerie van JenV. Portofoons zijn in ruime mate verkrijgbaar en geproduceerd door verschillende fabrikanten. Voor zover onderdelen voor zeer oude types portfoon niet meer verkrijgbaar zijn, kunnen deze portofoons vervangen worden als onderdeel van een regulier vervangingstraject.

De leden van de VVD-fractie vragen of het klopt dat Motorola en KPN, de leveranciers van C2000, hebben aangegeven dat de stabiliteit van C2000 na 2018 alleen gewaarborgd kan worden als er forse technologische updates plaatsvinden en zo ja, op welke manier geborgd is dat die noodzakelijke updates plaatsvinden nu Motorola en KPN vanaf 2019 niet meer betrokken zijn bij C2000. De leden van de VVD-fractie vragen op welke wijze de partijen die het beheer over C2000 vanaf januari 2019 over moeten nemen de stabiliteit van C2000 kunnen waarborgen.

De huidige leveranciers hebben aangegeven het C2000 netwerk na 2018 niet meer te ondersteunen zonder grote technologische updates. Ten behoeve van het onderhoud na 2018 is er daarom een contract gesloten met Nokia. Ten aanzien van de software geldt dat er geen software

wijzigingen worden doorgevoerd. Die zijn ook niet voorzien voor na 2018. In de afgelopen jaren hebben ook geen software wijzigingen plaatsgevonden. De huidige software functioneert stabiel en er is geen functionele noodzaak voor upgrades. Overigens blijft het Meldkamerdienstencentrum van de Politie het beheer van het C2000 netwerk uitvoeren. Het onderhoud, als onderdeel van beheer, wordt uitgevoerd door externe partijen.

Rol bureau Xebia

De leden van de VVD-fractie lezen in de brief van 26 april jl. dat de audits op het huidige C2000 die aan de basis staan van het oordeel dat C2000 robuust en stabiel is, zijn uitgevoerd door Xebia en vragen of het klopt dat Xebia ook de audits op het nieuwe C2000 uitvoert. Genoemde leden vragen of ik de mening deel dat het wenselijk is dat een partij die geen betrokkenheid heeft bij het nieuwe C2000 een dergelijke audit uitvoert en zo ja, of ik, mede op basis van de bevindingen van Zembla, bereid ben een nieuwe audit uit te laten voeren – zo nee, waarom niet.

Graag merk ik op dat Xebia geen betrokkenheid en belang heeft in de vernieuwing van C2000. Xebia heeft onafhankelijk onderzoek uitgevoerd naar de technische aspecten van het nieuwe C2000 netwerk, zoals de door de vernieuwingspartijen geleverde architectuur en de kwaliteit van de software. Voor de audit op het huidige C2000 systeem heeft Xebia de geschiktheid van het aanbod van de huidige leveranciers beoordeeld. Ik zie daarmee geen aanleiding voor een nieuwe audit.

4. Financiële consequenties

De leden van de CDA-fractie vragen of ik explicieter inzichtelijk kan maken welke incidentele extra uitgaven gedaan moeten worden en welke lagere uitgaven gerealiseerd worden als gevolg van de vertraging van de invoer van het vernieuwde C2000. Voornoemde leden vragen of ik dit kan expliciteren voor de jaren 2017, 2018 en 2019 waarbij inzichtelijk wordt gemaakt welke kostensoorten het betreft en welke bedragen daaraan gekoppeld zijn.

De leden van de SP-fractie verzoeken een overzicht van de totale kosten van C2000 tot nu toe, inclusief wat er eerst geraamd was.

Het beheer van het C2000 netwerk wordt jaarlijks gefinancierd als onderdeel van de rijksbijdrage «Beheer multisystemen», welke is opgenomen op artikel 31.3 van de begroting van het Ministerie van Justitie en Veiligheid. Het geraamde bedrag voor de multisystemen bedraagt jaarlijks circa € 100 mln. Over de besteding van deze middelen leg ik jaarlijks verantwoording af aan uw Kamer. Overigens wordt uit dit artikel ook het beheer van enkele andere meldkamersystemen bekostigd.

Het Meldkamerdienstencentrum van de politie (MDC) voert het beheer over C2000 uit. De beheerkosten bestaan naast organisatiekosten van MDC onder andere uit onderhoudscontracten voor het systeem, het conserveren van de masten, het periodiek bijplaatsen van masten, de groenvoorziening rond de masten, de toegangsbeveiliging tot de masten en contracten voor verschillende verbindingen.

Omdat was voorzien dat de vernieuwing van C2000 een aanzienlijke realisatietijd zou vergen is in 2013 eerst een aanbesteding uitgevoerd voor verlenging van het onderhoud op het huidige C2000-netwerk. Met deze aanbesteding zijn met ingang van medio 2014 besparingen met een omvang van ongeveer € 25 mln. per jaar gerealiseerd. Met deze besparing is ruimte in het beschikbare budget ontstaan om de vernieuwing van C2000 te kunnen financieren.

De raming van de totale kosten van de vernieuwing van C2000 bedroeg bij de start van het project circa € 167 miljoen. Dit bedrag bestaat uit een investering van circa € 127 miljoen en de raming van de kosten van het programma IVC van circa € 40 miljoen. De investeringskosten worden betaald aan de vernieuwingspartijen. Contractueel is afgesproken dat 75% hiervan moet zijn voldaan bij turn-key oplevering. De overige 25% komt tot betaling in de jaren van exploitatie van het systeem, tot aan 2027. Eind mei jl. was circa € 33 miljoen aan investeringskosten uitgegeven.

De kosten van het programma bestaan onder andere uit meerjarige personele- en huisvestingskosten, de kosten van de externe testinstantie en de opleidingskosten van de centralisten. Deze bedragen komen ter betaling in de jaren van de vernieuwing, gestart in 2015 en eindigend na het moment van de turn-key oplevering van het gehele nieuwe netwerk. Eind mei jl. was circa € 27 miljoen aan programmakosten uitgegeven.

In de contracten met de vernieuwingspartijen zijn tevens afspraken gemaakt over de exploitatie, het vierdelijns-onderhoud en de toekomstige exitkosten, van het nieuwe netwerk. Dit bedrag van circa € 50 miljoen is naast bovengenoemde bedragen opgenomen op het Rijksbrede ICT-dashboard en heeft betrekking op de jaren van het gebruik van het systeem. Dit start na de aangepaste planning nu niet eerder dan eind 2018 en eindigt nog steeds in 2027. Omdat het aantal jaren gebruik van het nieuwe netwerk hiermee korter is geworden zal het aantal jaarbedragen die in deze jaren contractueel betaald moeten worden voor de investeringen (25%) en exploitatie in het totaal ook lager zijn. Met een oplevering conform de huidige planning gaat het daarmee contractueel om ongeveer € 10 mln.

Voor het tweede- en derdelijns-onderhoud van het nieuwe C2000 netwerk is na aanbesteding een contract gesloten met Koning en Hartman. Een optelling van alle contracten voor het nieuwe C2000 netwerk leidt tot significant lagere jaarlijkse totale beheerkosten dan het huidige netwerk. Concluderend blijven de financiële consequenties van de vernieuwing binnen het meerjarig budgettair kader dat beschikbaar is voor het gebruik van het huidige en nieuwe C2000 netwerk. In het totaal van gebruiksjaren bezien leidt de vernieuwing van C2000 nog steeds tot een besparing. Deze besparing start nu in een later jaar. Bij het meest gunstige scenario van de vernieuwing zou de cumulatieve besparing maximaal zijn uitgevallen, maar in een zo complex traject met zoveel onderlinge afhankelijkheden moet rekening worden gehouden met risico's en daarbij behorende mitigerende maatregelen. Het maximale besparingsscenario is nooit een doel op zich geweest, we streven immers naar een kwalitatief hoogwaardig netwerk voor onze hulpverleners.

5. Toekomstig mobiel breedband voor de OOV-diensten

De leden van de D66-fractie lezen dat momenteel wordt bezien op welke wijze invulling gegeven kan worden aan de toekomstige behoefte aan mobiel breedband voor communicatie in de OOV-sector en constateren dat dergelijk mobiel breedband in eerste instantie naast C2000 zal bestaan, om vervolgens de primaire communicatievorm te worden voor de sector. Voornoemde leden vragen waarom ik het noodzakelijk en proportioneel acht dat ondanks het feit dat het nieuwe C2000-systeem nog niet is ingevoerd, al wel een traject in gang wordt gezet naar een systeem waarin mobiel breedband de primaire communicatievorm wordt en of het in dit geval niet mogelijk en logischer is om vanaf het huidige C2000 systeem direct over te stappen naar een dergelijk nieuw communicatiesysteem.

Voorafgaand aan de aanbesteding van de vernieuwing van C2000 heeft mijn ministerie TNO gevraagd een advies uit te brengen over de te kiezen technologie. De keuze was daarbij om door te gaan met de inmiddels «proven» TETRA-technologie of al over te gaan op 4G/5G technologie. TNO heeft daarbij geadviseerd om nog verder te gaan met de TETRA-technologie, omdat de ontwikkeling van de OOV communicatie op 4G nog onvoldoende volwassen was. Dat is overigens ook op dit moment nog steeds het geval. Zoals ik in mijn brief van 26 april 2018 aan uw Kamer heb gemeld, is het gebruik van mobiel breedband voor missiekritische communicatie nog onvoldoende ontwikkeld om op korte termijn als een bewezen alternatief voor TETRA te kunnen beschouwen. Daarom is gekozen voor de huidige *midlife upgrade* van het bestaande C2000 netwerk met een verlenging van de technische levensduur met ongeveer 8 tot 10 jaar. Ondertussen wordt voor de toekomst geanticiperd op de ontwikkelingen van 4G en inmiddels ook 5G. In andere Europese landen wordt momenteel dezelfde ontwikkeling doorlopen.

TETRA-technologie is primair gericht op spraak en kan slechts in beperkte mate data verzenden. De OOV-sector heeft echter in toenemende mate behoefte aan dataverkeer, zoals het streamen van beelden, locatie- of objectgegevens en snelle online database bevestigingen. Dergelijk dataverkeer zal ook in toenemende mate missiekritisch worden. Dit brengt een andere behoefte voor de noodhulpcommunicatie met zich mee. Daarom moet, naast de migratie naar het vernieuwde C2000 netwerk, ook al verder vooruit gekeken worden. Overigens zie ik ook de beveiliging van deze 4G/5G technologie voor missiekritische en vitale communicatie in de toekomst als een issue.

De leden van de D66-fractie vragen welke kosten gemoeid zijn met het voorgestelde onderzoek naar het gebruik van mobiele breedband voor missiekritische communicatie?

In mijn brief van 26 april 2018 heb ik uw Kamer gemeld dat ik, in samenspraak met de Staatssecretaris van Economische Zaken en Klimaat, in de komende periode ga bezien op welke wijze deze ontwikkeling gezamenlijk met de markt verkend kan worden, ook in de context van vergelijkbare ontwikkelingen in het andere Europese landen. Dit is nog niet in een dermate concreet stadium dat het al aan de orde is om hiervoor de kosten in te schatten.

6. Nieuwe meldkamers

De leden van de D66-fractie zijn benieuwd of de nieuwe meldkamer in Rotterdam inmiddels als eerste samengevoegde meldkamer is aangesloten op de landelijke ICT-voorziening voor het meldkamerdomein. De meldkamer in Rotterdam is inderdaad medio mei als eerste samengevoegde meldkamer aangesloten op de landelijke ICT-voorziening.

De leden van de D66-fractie vragen hoeveel vertraging het in gebruik nemen van de meldkamer in Rotterdam in totaal heeft opgelopen. De opening van de nieuwe meldkamer in Rotterdam was eerst voorzien op 8 augustus 2017 en vervolgens medio november 2017.

De leden van de D66-fractie vragen of het nog steeds de planning is dat de meldkamers in Den Bosch en Haarlem volgend jaar volgen en hoeveel vertraging het in gebruik nemen van deze meldkamers in totaal heeft opgelopen.

In de huidige planning zal Den Bosch eind 2018, na de migratie van C2000, worden aangesloten op de landelijke ICT-voorziening en Haarlem begin 2019. Beide meldkamers hadden dit enkele maanden eerder beoogd.

De leden van de SP-fractie vragen een reflectie op het proces van het samenvoegen van de meldkamers, nu niet in 2020 maar in 2021 het doel wordt gehaald en vragen of ik de mening deel dat een reorganisatie van dit formaat niet samen gaat met een bezuiniging van deze omvang en zo nee, wat volgens mij dan de reden is dat dit proces zoveel moeilijkheden kent.

Meldkamers vormen een vitale voorziening in onze maatschappij, die 24/7 beschikbaar is voor burgers en hulpdiensten en waarbij elke seconde telt. Veranderingen in deze complexe omgeving vragen om een zeer zorgvuldig voorbereiding en uitvoering, van de verschillende verantwoordelijken. Naast een nieuw ingerichte meldkamer en goed toegerust personeel vormt de beschikbare huisvesting en ICT-capaciteit een belangrijke randvoorwaarde om zowel de continuïteit van de meldkamer als de samenvoeging te kunnen realiseren. De combinatie hiervan vormt de voornaamste reden dat laatste samengevoegde meldkamer na 2020 gerealiseerd zal worden.

De beschikbare financiële middelen vormen geen doorslaggevende factor voor het tempo van de samenvoegingen. Begin 2017 heb ik laten onderzoeken, op basis van de thans bestaande inzichten, of de voorziene structurele besparing van € 50 miljoen op het meldkamerdomein nog haalbaar is. Het onderzoek maakt op basis van de nu beschikbare informatie de inschatting dat de veronderstelde besparing op personele inzet op termijn te realiseren moet zijn. Het onderzoek signaleert daarbij wel een risico ten aanzien van de structurele besparing op materiële kosten, voornamelijk huisvesting en ICT.

Eerder dit jaar heb ik met partijen bestuurlijke overeenstemming bereikt over het Uitwerkingskader Meldkamers. Daarin heb ik een voorstel gedaan dat op een drietal onderwerpen helderheid biedt: de hoofdlijnen van de wetswijziging, de nieuwe werkwijze van de meldkamers en afrondende financiële afspraken over de toekomstige bekostiging van het beheer van de meldkamers door de politie.

In deze complexiteit met vele verwevenheden en afhankelijkheden, is het voor vitale organisaties en systemen als meldkamers en C2000 nooit uit te sluiten dat plannings moeten worden aangepast. De afgelopen jaren, maar zeker ook de komende jaren, zullen nog vele veranderingen en vernieuwingen op het meldkamerdomein plaatsvinden, met vele betrokken partijen: bestuurlijk en operationeel, landelijk en regionaal. Er zijn daarbij vele afhankelijkheden waarop steeds door alle betrokken partijen zo goed als mogelijk integraal wordt gestuurd.

6. Stand van zaken 112

Persinformatie 112-meldingen

De leden van de CDA-fractie vragen of ik de stelling deel dat het vernieuwde C2000 journalisten nagenoeg onmogelijk maakt om kennis te nemen van actuele activiteiten van hulpdiensten, de politie in het bijzonder. Voornoemde leden vragen of ik de mening deel dat hiermee de mogelijkheden van journalisten om verslag te doen tot een minimum worden teruggebracht. Voornoemde leden vragen of ik het standpunt deel dat vrije nieuwsgaring ook bij digitaal dataverkeer tussen hulpverleners tot de mogelijkheden moet blijven behoren. Deze leden vragen of ik kan aangeven op welke wijze de persvrijheid – met name die voor fotojournalisten – vanuit de politie gefaciliteerd wordt.

In 2016 heeft de CDA-fractie mijn ambtsvoorganger gevraagd of deze de mening deelde dat privacygevoelige informatie van 112-meldingen niet

gepubliceerd hoort te worden³⁶. Mijn ambtsvoorganger heeft die vraag destijds bevestigend beantwoord en ook ik deel deze mening. Veel 112-meldingen bevatten informatie aan de hand waarvan natuurlijke personen kunnen worden geïdentificeerd. Een adresgegeven bijvoorbeeld is herleidbaar tot een persoon die op dat adres woonachtig is; de soort inzet en de prioriteit daarvan kunnen een indicatie geven over de bijzondere omstandigheden waarin die bewoner verkeert, waaronder zijn fysieke of mentale gezondheid. Dergelijke privacygevoelige gegevens behoren niet via een algemeen toegankelijke informatiebron openbaar te worden gemaakt. In zulke gevallen dient naar mijn oordeel de bescherming van de persoonlijke levenssfeer van degenen op wie de informatie betrekking heeft te prevaleren boven het recht op vrije nieuwsgaring van de media. Ik zal de hulpverleningsdiensten verzoeken hun afspraken met de media opnieuw te bezien in het kader van de vernieuwing van C2000.

De leden van de CDA-fractie vragen of ik bereid ben een verkennende studie te laten verrichten over hoe in andere landen omgegaan wordt met de informatievoorziening rond actuele gebeurtenissen, vanuit de hulpverleningsdiensten wiens dataverkeer volledig gedigitaliseerd is. Ik acht het niet opportuun om hier een verkennende studie voor te starten. Wel kan ik in mijn bilaterale contacten informeren naar de praktijk in andere landen op dit terrein. Overigens plaats ik dit onderwerp nadrukkelijk in het licht van de EU-brede implementatie van de Algemene Verordening Gegevensbescherming (AVG).

Mobiel bereik 112

De leden van de SP-fractie vragen of er nu gegarandeerd kan worden dat ook in gebieden waar slecht mobiel bereik is, de bereikbaarheid van 112 wel gewaarborgd is.

Zoals ik uw Kamer in april jl. gemeld heb³⁷ naar aanleiding van mondelinge vragen van het lid Van Toorenburg (CDA) tijdens het vragenuur van 23 januari 2018, is er de afgelopen jaren op verschillende manieren gewerkt aan het verder verbeteren van de mobiele bereikbaarheid van 112 (Handelingen II 2017/18, nr. 42, item 5). Gemeenten en operators hebben acties genomen en verbeteringen doorgevoerd en ik heb er vertrouwen in dat deze partijen hun verantwoordelijkheid zullen blijven nemen bij het verbeteren van de mobiele bereikbaarheid van 112.

7. Diversen

Door Zembla gesuggereerd spreekverbod

De leden van de D66-fractie vragen of het klopt dat het Ministerie van Justitie en Veiligheid iedereen die meewerkt aan C2000 verboden heeft om met Zembla te spreken naar aanleiding van de uitzending over C2000 en zo ja, waarom.

Nee, dit is onjuist. Het Ministerie van Justitie en Veiligheid heeft niemand verboden om met Zembla te spreken.

Samenwerking in de grensstreken met België en Duitsland

De leden van de ChristenUnie-fractie constateren dat in de grensregio het knelpunt bestaat dat samenwerkende Veiligheidsregio's in Nederland, Duitsland en België verschillende communicatiesystemen in de voertuigen (zoals de brandweerauto's) hanteren, waardoor snelle en

³⁶ Aanhangsel Handelingen II 2016/17, nr. 1050

³⁷ Kamerstuk 29 628, nr. 773

directe communicatie wordt bemoeilijkt bij calamiteiten. Zeker bij een grote calamiteit moeten politie, brandweer en ambulancediensten kunnen vertrouwen op directe en ongehinderde communicatie. Voornoemde leden vragen op welke manier rekening wordt gehouden met samenwerkende Veiligheidsregio's in de grensregio bij het huidige C2000-systeem en bij de verdere ontwikkeling van het C2000-systeem. Voornoemde leden vragen hoe nu en in de toekomst directe en ongehinderde communicatie wordt gegarandeerd tussen de Nederlandse, Duitse en Belgische hulpverleningsdiensten.

Aanvullend op deze vragen heeft uw Kamer ook de motie Van der Graaf c.s. aangenomen³⁸, waarin de regering wordt verzocht om met een oplossing te komen voor het probleem van verschillende communicatiesystemen van Nederlandse, Duitse en Belgische hulpverleningsdiensten, waardoor snelle en directe communicatie wordt bemoeilijkt, en de Kamer hierover voor de begrotingsbehandeling te informeren. Met deze beantwoording van de schriftelijke inbreng informeer ik tevens uw Kamer conform deze motie.

Allereerst is het inrichten van de communicatiesystemen voor de hulpdiensten een nationale verantwoordelijkheid. Nederland, België en Duitsland hebben elk hun eigen systeem, respectievelijk C2000, ASTRID en Digitalfunk BOS, die allen gebaseerd zijn op de TETRA technologie. In de grensoverschrijdende samenwerking van de hulpdiensten zijn er meerdere knelpunten die andersoortige oplossingen vergen en waarover het gesprek met beide landen gevoerd moet worden.

Binnen 10km over de grens, wens om binnen het eigen netwerk te kunnen communiceren met de andere hulpdienst.

Binnen de eerste 10 km over de grens is er nog bereik van het eigen netwerk. De Nederlandse hulpdiensten kunnen dan dus nog gebruik maken van C2000, en mutatis mutandis geldt hetzelfde voor de Duitse en Belgische hulpdiensten. In de operatie bestaat grote behoefte om in de strook van 10 km aan weerszijden van de grens, te kunnen communiceren met beide netwerken, zodat hulpverleners en meldkamers over en weer zowel op eigen grondgebied als aan de andere kant van de grens kunnen communiceren.

Technische oplossing hiervoor is om over en weer een aantal gespreksgroepen op elkaars systeem aan te maken. Gespreksgroepen moeten vooraf worden voorbereid en vóór een daadwerkelijke inzet worden ingeschakeld. De vastgestelde gespreksgroepen van de desbetreffende landen zijn met elkaar verbonden. Dit betekent dat radioberichten in de gespreksgroepen aan Duitse zijde ook in het Nederlandse net uitgezonden worden. Portofoons die binnen een dergelijke gespreksgroep zijn opgenomen, kunnen communiceren met alle portofoons binnen die gespreksgroep en ontvangen alle berichten binnen die gespreksgroep. Voorwaarde is dat de portofoon binnen het bereik van het eigen netwerk valt. Dat is binnen een straal van tien tot vijftien kilometer van de grens. Bij een daadwerkelijke inzet over de grens volstaat dat in de meeste gevallen.

Met zowel België als Duitsland is dit concept technisch reeds geïmplementeerd (benaming respectievelijk KTS en EUCOM).

Meer dan 10 km over de grens, wens om te kunnen overschakelen naar het andere netwerk omdat het eigen netwerk mogelijk geen bereik meer heeft.

Vanaf ca. 10 tot 15 km voorbij de grens kan de verbinding met het eigen netwerk uitvallen. Dit kan leiden tot gevaarlijke situaties én verlies van

³⁸ Kamerstuk 32 851, nr. 42 (naar aanleiding van het Algemeen Overleg Grensoverschrijdende Samenwerking d.d. 25 april 2018, Kamerstuk 32 851, nr. 47).

heterdaadkracht. Hiervoor bestaan meerdere oplossingen. Een structurele technische oplossing, zij het kostbaar, zou de zogeheten ISI zijn, een interface om twee individuele TETRA-netwerken aan elkaar te koppelen zodat roaming mogelijk wordt net zoals bij een gsm netwerk. Echter, in verband met de lopende vernieuwing van het C2000 netwerk, zou deze oplossing pas op zijn vroegst vanaf (medio/eind) 2020 kunnen worden ingevoerd. In afwachting van ISI als structurele oplossing is er een praktische tussenoplossing mogelijk. Dit wordt de *semi-roaming* oplossing genoemd. Dit houdt in het kruislings geschikt maken van een aantal portofoons voor elkaars netwerk (deze optie wordt nu al op kleine schaal toegepast bij wielerevenementen in de grensstreek met België). Met de Belgische Minister van Binnenlandse Zaken Jambon ben ik over de semi-roaming oplossing in gesprek en blijf daarbij aandringen op een spoedige invoering van deze oplossing. Met Duitsland was het gesprek over de semi-roaming oplossing in een vergevorderd stadium met de betreffende deelstaten. Echter, onlangs heeft het Duitse federale ministerie zich op het standpunt gesteld dat zij geen externen willen toelaten op Digitalfunk BOS. Voor dit moment ligt de ontwikkeling dus stil. Het is mij nog niet bekend of dit ook consequenties heeft voor de EUCOM oplossing zoals hierboven beschreven. Ik zal zeker met mijn Duitse collega het gesprek aangaan over de mogelijkheid om toch tot een semi-roaming oplossing te komen.