Haalbaarheidsonderzoek naar de toekomst van missiekritische breedbandcommunicatie in Nederland

versie 1.0, 9 juni 2020

Colofon

Documentnaam	MinJenV haalbaarheidsonderzoek missiekrit.communicatie.doc
Titel	Haalbaarheidsonderzoek Toekomst Missiekritische Breedband Communicatie in NL
Referentienummer	202001-5687-1
Versie, datum	Versie 1.0, 9 juni 2020
Samengesteld door	Rick de Rooij; Joost Beukers; Gert-Jan Elzinga; Antoine van der Sijs
Project	HBO-JenV

Contactadres voor deze publicatie

Strict Consultancy

Lange Dreef 11-f

4131 NJ Vianen

Postbus 12

4130 EA Vianen

INHOUDSOPGAVE

MANAGEMENT SAMENVATTING

In opdracht van het ministerie van Justitie en Veiligheid hebben Strict en VKA een onderzoek uitgevoerd naar de haalbaarheid om vanaf 2025 missiekritische communicatie te realiseren over een mobiel breedbandnetwerk (4G/5G en verder). Het onderzoek is begeleid door een begeleidingscommissie die bestaat uit vertegenwoordigers van de ministeries van VenJ, EZK en Defensie, van de Nederlandse politie, de veiligheidsregio's, ambulancediensten en TNO (als kennispartner).

De hulpdiensten in Nederland maken momenteel gebruik van het C2000-netwerk. Dat netwerk is gebaseerd op de TETRA-standaard en wordt in veel landen gebruikt als netwerktechnologie voor missiekritische *spraak*communicatie. Het belang van breedbandige *data*communicatie neemt echter fors toe, voor toepassingen als het direct online raadplegen van databases, het doorsturen van live beelden van bodycams en het gebruik van allerlei apps. Door de beperkingen van de onderliggende technologie kan het huidige C2000 daar nu niet in voorzien. Hulpdiensten maken nu al wel gebruik van mobiele devices, maar die datacommunicatie loopt via de 3G/4G-netwerken van de mobiele operators in Nederland. Dit gebruik is op basis van 'best-effort'; er zijn geen prioriteitsafspraken gemaakt om te voorkomen dat bij grote drukte of een calamiteit de verbinding uitvalt.

Het ministerie heeft de strategische keuze gemaakt om aansluiting te zoeken bij de standaarden die door de 3GPP-organisatie worden opgesteld. 3GPP is een samenwerking tussen zeven internationale standaardisatieorganisaties om standaarden te ontwikkelen voor de doorontwikkeling van mobiele GSM-netwerken. Binnen de 3GPP-organisatie is een werkgroep actief om standaarden te ontwikkeling specifiek voor missiekritische toepassingen. Op dit moment van dit onderzoek (juni 2020) is de standaard voor missiekritische communicatie nog in ontwikkeling. Voor 4G zijn de eerste releases van MCX-functies gebaseerd op de releases 13, 14 en 15 inmiddels beschikbaar. Echter, niet alle functies die in de TETRA-standaard zijn opgenomen, zijn op een vergelijkbaar missiekritisch niveau beschikbaar in deze releases.

De standaardisatie-ontwikkeling van de MCX-functionaliteiten over een 5G-netwerk moeten nog starten en zullen pas vanaf release 17 beschikbaar komen. Release 17 wordt volgens de huidige planning in december 2021 uitgebracht. De verwachting is dat missiekritische MCX-functies niet vóór 2024 op een operationeel 5G-netwerk mogelijk zijn.

Dat betekent dat nu niet met zekerheid gesteld kan worden dat er in 2025 een commercieel aanbod is vanuit operators op basis van een standaard die voldoet aan de eisen van de Nederlandse overheid, zoals op het gebied van functionaliteit, bandbreedte en beveiliging. Dat is een risico, maar gezien de snelheid waarmee de standaardisatie wordt opgepakt en het gegeven dat veel andere landen ook gekozen hebben voor 3GPP-standaarden, zien wij op dit moment geen reden waarom de overheid zou moeten afwijken van de (voorlopige) richting zoals verwoord in de Tweede Kamer-brief van november 2019[1].

Voor het onderzoek is een vergelijking gemaakt tussen een drietal scenario's. Hierbij is gekozen voor twee scenario's waarin de uitersten tot hun recht komen en een derde scenario tussen deze uitersten in. De ratio hierachter is dat het onderzoek inzicht moet geven in de *haalbaarheid* van het gebruik van mobiele breedband technologie, niet in de exacte specificaties van het optimale scenario. De scenario's zijn:

[1] Brief van de minister van Justitie en Veiligheid aan de Tweede Kamer van 12 november 2019 met kenmerk 2730330.

1. **Volledig eigen beheer**: de overheid heeft, met uitzondering van het transmissienetwerk, het volledige mobiele breedband netwerk voor missiekritische communicatie aangeschaft (in eigendom verkregen, inclusief eigen frequentiespectrum) en voert zelf het beheer over dit netwerk.
2. **Volledig uitbesteed**: De overheid neemt het mobiele breedband netwerk als dienst af van MNO's (Mobiele Netwerk Operators) op basis van nader af te spreken tarieven en dienstniveau.
3. **Gedeeltelijk uitbesteed**: De overheid heeft in dit scenario het core-netwerk in eigendom (en beheer) en het radionetwerk en het transmissienetwerk is uitbesteed aan één mobiele operator op basis van nader af te spreken tarieven en dienstniveau.

De scenario's zijn vergeleken met elkaar én met het huidige C2000-netwerk op dertien criteria (en ongeveer 50 subcriteria) waaronder de mate van strategisch/politieke zeggenschap, techniek, beveiliging, organisatie, internationale ontwikkelingen, toekomstvastheid en financiën.

Een netwerk voor missiekritische communicatie kent een strategisch belang en vormt een essentiële én onmisbare voorziening voor de OOV-organisaties. Het voordeel van het scenario Volledig eigen beheer is de maximale strategische en politieke invloed op de oplossing, de volledige zeggenschap over de beveiliging van de oplossing, binnen de kaders die de gekozen apparatuur biedt en de hoge mate van leveranciersonafhankelijkheid. De overheid heeft (binnen de grenzen van de aanbestedingswetgeving) de ruimte om zelf te bepalen op basis van welke technologie zij haar netwerk bouwt, welke leverancier(s) componenten mogen leveren en welke dienstverleners ze inhuurt. Let wel, ook in dit scenario blijft er voor de overheid een afhankelijkheid van leveranciers bestaan; volledig onafhankelijk zou alleen kunnen als de overheid zelfstandig de noodzakelijke apparatuur en software ontwikkelt en produceert. Dat is te complex, te kostbaar en niet haalbaar.

Een netwerk in eigen beheer (scenario 1) achten wij echter **niet haalbaar** om de volgende redenen:

- Er zijn grote investeringen en operationele lasten gemoeid met dit scenario. De high level financiële vergelijking laat zien dat het grofweg tweemaal zo duur is als de scenario's van uitbesteden.
- Een eigen netwerk opbouwen vergt een veel langere doorlooptijd, met name om voldoende antenne-opstelpunten en transmissielijnen te realiseren.
- Er is, met instemming van het ministerie van JenV, nu onvoldoende spectrum gealloceerd in het Nationale Frequentieplan (NFP) voor een eigen overheidsnetwerk. Het is op dit moment vrijwel onmogelijk om genoeg aanvullend spectrum beschikbaar te krijgen omdat geschikt frequentiespectrum reeds toegewezen is aan andere partijen.
- De overheid beschikt op dit moment niet over een eigen netwerkoperator voor breedbandnetwerken. Dat betekent dat alle kennis en personeel moet worden verworven in een markt waar deze mensen schaars zijn. Er is binnen de overheid wel kennis en ervaring met C2000 aanwezig, maar niet met mobiel breedband.

Het tweede scenario **Volledig uitbesteed** heeft als voordeel dat de overheid in veel mindere mate eigen technische en operationele expertise hoeft te verwerven en dat meegelift kan worden op de bestaande en nieuw aan te leggen infrastructuren van de MNO's. Dat verkort de doorlooptijd met enkele jaren. Door aan te sluiten op de radionetwerken van alle MNO's wordt extra redundantie in het radionetwerk verkregen, is er potentieel een grotere capaciteit bij calamiteiten beschikbaar (dit vergt nadere afspraken over prioriteit van verkeer) en is er aldus een betere beschikbaarheid. Voor de beveiliging is de overheid afhankelijk van de keuzen die de operators maken en de mogelijkheid om aanvullende afspraken te maken.

Het derde scenario **Gedeeltelijk uitbesteed** biedt voordelen op de punten van zeggenschap, onafhankelijkheid en beveiliging omdat het core-netwerk in eigendom en beheer van de overheid is. De kosten van het core-netwerk zijn relatief laag in vergelijking met de kosten van het totale netwerk. Uit de financiële vergelijking komt naar voren dat het core-netwerk ongeveer 4% van de totale kosten van een compleet mobiel breedbandnetwerk vertegenwoordigt. Voor deze relatief lage kosten krijgt de overheid een aanzienlijke controle over het totale netwerk.

In de detailvergelijking ‘scoort’ scenario 2 net iets beter dan scenario 3, met name op de criteria techniek (dekking, beschikbaarheid en piekcapaciteit), organisatie (kennis en ervaring van de operators) en lagere risico’s (kleinere kans op marktverstoring, gebruik maken van core-netwerk operator geeft lager operationeel risico). Om een definitieve afweging tussen de scenario’s en eventuele tussenliggende varianten te kunnen maken, moeten in de komende periode verschillende verdiepingsslagen gemaakt worden. De uitkomst van de verdiepingsslagen geeft aan of bepaalde criteria zwaarder of juist lichter moeten wegen, of dat aanvullende maatregelen nodig zijn om een scenario te kunnen realiseren.

Een eerste analyse wijst in de richting van een variant waarbij de overheid wel een eigen core-netwerk heeft (zoals in scenario 3), maar gebruik maakt van de radionetwerken van alle drie de Nederlandse operators. Hiermee verkrijgt de overheid op een kostenefficiënte manier veel controle over beveiliging, toegang en functionaliteit en is er een optimale dekking, gebruik van spectrum, capaciteit, internationale samenwerking en mogelijkheden voor fallback bij storingen. Mogelijke risico’s zitten vooral in de technische complexiteit en het verkrijgen van voldoende inhoudelijke expertise binnen de overheid.

In het bepalen van de ‘routekaart’ voor de komende jaren speelt de in het begin van dit hoofdstuk al genoemde standaardisatie-ontwikkeling een belangrijke rol. Het risico dat de markt niet tijdig de vanuit missiekritische toepassingen gewenste releases aanbiedt, kan beperkt worden door het huidige C2000-netwerk parallel naast de missiekritische mobiele breedbandoplossing (in ontwikkeling) operationeel te houden. De mobiele breedbandoplossing kan dan gefaseerd ingericht worden, waarbij de kosten beperkt worden door de eisen af te stemmen op het actuele gebruik en de kostenconsequenties.

Een belangrijke stap is om samen met de operators na te gaan of de technische complexiteit van een oplossing met alledrie de operators kan worden bedwongen om te verifiëren of dit een voor alle partijen werkbare oplossing is.

De conclusie op de vraag of het haalbaar is om vanaf 2025 missiekritische communicatie te realiseren over een op 3GPP-gebaseerd mobiel breedbandnetwerk luidt, dat we op basis van de huidige kennis en inzichten die oplossingsrichting inderdaad haalbaar achten. Omdat er nog steeds onzekerheden en ontwikkelingen zijn waar de komende jaren meer inzicht in zal komen, bevelen wij aan om uiterlijk over twee jaar, maar vóór de aanbesteding wordt gestart, een herijking van dit onderzoek uit te voeren. Daarbij zal niet de fundamentele keuze voor de 3GPP-oplossingsrichting ter discussie staan, maar vooral de detailkeuzes binnen die oplossingsrichting.

1 INLEIDING

1.1 Algemeen

Communicatie tussen en binnen hulpdiensten in geval van incidenten of crisissituaties (hierna: *missiekritische communicatie*) is van levensbelang. Het ministerie van Justitie en Veiligheid (JenV) draagt zorg voor de voorzieningen die nodig zijn om deze communicatie mogelijk te maken. Door de ontwikkeling in mobiele breedbandcommunicatie ontstaan nieuwe gebruiksmogelijkheden zoals video en data voor missiekritische communicatie.

De hulpdiensten in Nederland maken momenteel gebruik van het C2000-netwerk. In de afgelopen jaren heeft het project IVC (Implementatie Vernieuwing C2000) de basis gelegd voor de vernieuwing van het C2000-netwerk en recent heeft de migratie naar het nieuwe (Hytera) netwerk plaatsgevonden. Het IVC-netwerk is - net als het oorspronkelijke C2000-netwerk - gebaseerd op de TETRA-standaard: deze standaard ondersteunt in het bijzonder missiekritische *spraak*communicatie. TETRA staat voor Terrestrial Trunked Radio.

Minister Grapperhaus van Justitie en Veiligheid heeft in 2019 naar aanleiding van diverse onderzoeken in het overleg met de Tweede Kamer aangegeven, dat, parallel aan de uitrol van het nieuwe C2000 netwerk, zo snel mogelijk de verkenning start voor de aanbesteding van een vervangingstraject. Een eis is dat de afhankelijkheid van landen met een offensief cyberprogramma gericht tegen Nederlandse belangen wordt geminimaliseerd.

Daarnaast wordt de behoefte aan breedbandige communicatie ook binnen de processen van de hulpdiensten steeds groter en derhalve heeft de minister in de brief van 12 november 2019 aan de Tweede Kamer aangekondigd[2]:

'een haalbaarheidsonderzoek te willen laten uitvoeren over de toekomst van missiekritische communicatie, waarin de voor- en nadelen van de verschillende modellen voor missiekritische communicatie gebaseerd op mobiel breedband in beeld worden gebracht. Daarbij wordt een vergelijking gemaakt met de huidige situatie'.

Het ministerie van JenV heeft aan de combinatie Strict/VKA de opdracht verstrekt om de haalbaarheid te onderzoeken en het ministerie hierover te adviseren.

Binnen het DGP&V van het ministerie van JenV is een projectorganisatie opgezet. De projectleider van de projectorganisatie treedt op als opdrachtgever voor het haalbaarheidsonderzoek. De projectorganisatie wordt begeleid door een begeleidingsgroep bestaande uit vertegenwoordigers van de ministeries van VenJ, EZK en Defensie, van de Nederlandse politie, de veiligheidsregio's, ambulancediensten en TNO (als kennispartner). Het voorzitterschap van de begeleidingsgroep is belegd bij het ministerie van Justitie en Veiligheid.

In deze rapportage is het onderzoek en het onderzoeksresultaat beschreven.

1.2 Vraagstelling opdrachtgever

De opdrachtgever heeft de volgende onderzoeksvragen c.q. -opdrachten geformuleerd:

- Maak inzichtelijk welke scenario's er mogelijk zijn aangaande het gebruik van mobiele breedband communicatie in de missiekritische communicatie en welke voor- en nadelen deze scenario's hebben.
- Voorzie de uitwerking van een advies ten aanzien van het te prefereren toekomstscenario. Het advies dient een robuuste onderbouwing te bevatten, zodat dit kan worden gebruikt bij het advies aan de minister van

[2] Brief van de minister van Justitie en Veiligheid aan de Tweede Kamer van 12 november 2019 met kenmerk 2730330.

JenV. Het rapport zal door het projectteam van het ministerie worden gebruikt ter onderbouwing van een voorgenomen besluit. Het geheel zal deel gaan uitmaken van een brief aan de Tweede Kamer (voorzien in juli 2020).

1.3 Doelstelling onderzoek

Het haalbaarheidsonderzoek heeft als doel om de oplossingsrichting van missiekritische communicatie in Nederland op hoofdlijnen te duiden en de voorlopige keuze hiervoor te onderbouwen. Het onderzoek heeft niet als doel om tot in details de beoogde communicatievoorziening te specificeren; dat kan in een later stadium plaatsvinden.

1.4 Afbakening

De afbakening van het haalbaarheidsonderzoek is in overleg met de opdrachtgever vastgesteld. Deze vastgestelde reikwijdte is hieronder weergegeven.

Binnen de reikwijdte van het onderzoek vallen de volgende aspecten:

- Het onderzoek betreft de missiekritische communicatie, waarvoor het ministerie van JenV verantwoordelijk is, zoals toegepast binnen de hulpdiensten als ook tussen hulpdiensten onderling en met de meldkamers, in geval van incidenten en/of crisissituaties.
- Het ministerie heeft de keuze gemaakt dat de missiekritische communicatie gebaseerd wordt op de 4G- en/of 5G-standaarden van de standaardisatie organisatie 3GPP. Hierin zijn zowel bepalingen voor generieke dienstverlening als ook voor missiekritische toepassingen opgenomen.
- Het mobiele breedband communicatienetwerk-gedeelte valt binnen de scope van het onderzoek. Het mobiele breedbandnetwerk-gedeelte start vanaf het draadloze interfacevlak tussen het mobiele randapparaat (device) en de antennemast van het mobiele netwerk tot aan het interfacevlak naar andere netwerken of toepassingen/applicaties. In de figuur 2. in paragraaf 2.4.1 zijn de technische onderdelen, die binnen de scope van het onderzoek vallen schematisch getekend binnen de lichtblauwe rechthoek.
- De netwerkfuncties van de missiekritische standaarden vallen binnen de scope van het onderzoek. 3GPP standaardiseert missiekritische functies: MC PTT (spraak), MC Data en MC Video. Samengevat worden deze functies MCX genoemd.
- De koppelvlakken naar externe netwerken, bijvoorbeeld roaming koppeling met andere mobiele breedbandnetwerken of koppeling met het internet of private vaste netwerken, die binnen 3GPP gedefinieerd zijn, vallen binnen de scope van het onderzoek. Zie de figuur in paragraaf 2.4.1.
- Het koppelvlak tussen het radionetwerk en de mobiele randapparatuur, zoals binnen 3GPP is gedefinieerd (zowel voor 4G als 5G), valt binnen de scope van het onderzoek.
- De huidige C2000-inrichting is onder de noemer 0-scenario als referentiescenario meegenomen in het onderzoek.

Buiten de reikwijdte van het onderzoek vallen:

- Andere missiekritische communicatie van het ministerie van JenV of van de overheid in het algemeen valt buiten de scope van dit onderzoek. Zoals bijvoorbeeld de 112-communicatie, de communicatie binnen en tussen de meldkamers (voor zover dat niet-draadloos plaats vindt), et cetera.
- Andere mobiele communicatietechnologieën dan mobiele breedbandtechnologie volgens de 3GPP-definitie, vallen buiten de scope van het onderzoek, met uitzondering van de huidige C2000-inrichting.
- De missiekritische MCX-applicatiefuncties en de daarvoor benodigde platformen vallen buiten de reikwijdte van het onderzoek.

- Andere toepassingen en gebruikersapplicaties dan de missiekritische toepassingen gestandaardiseerd door 3GPP, vallen buiten de scope van dit onderzoek, zoals bijvoorbeeld meldkamerapplicaties.
- De mobiele randapparatuur en de accessoires van de randapparatuur vallen buiten de scope van het onderzoek.
- Andere netwerken dan de door 3GPP gedefinieerde mobiele breedbandnetwerken vallen buiten de scope van het onderzoek (zoals bijvoorbeeld het internet, het openbare vaste telefonienetwerk).

1.5 Leeswijzer

Het onderzoek is op basis van de multicriteria analyse opgezet. In hoofdstuk 2 staat de opzet van het onderzoek beschreven, wordt uitleg gegeven over de methodiek en de gekozen toekomstscenario's. In hoofdstuk 3 is de huidige situatie geschetst en zijn de ontwikkelingen weergegeven op diverse vlakken: de technologie, beveiliging, nationaal, en internationaal. Hoofdstuk 4 gaat in op het onderzoek en de resultaten zijn in hoofdstuk 5 opgenomen. Naast de resultaten van de kwalitatieve criteria beoordeling zijn ook de resultaten van de financiële vergelijking, de voor- en nadelen per scenario en de risico's in dit hoofdstuk opgenomen. De conclusies en aanbevelingen staan respectievelijk beschreven in de hoofdstukken 6 en 7. In de bijlagen is een overzicht opgenomen van de verklaring van afkortingen, de brondocumenten, detailuitwerking van de criteria met de scores en onderbouwing per scenario en de financiële vergelijking.

1.6 Definities en brondocumenten

De definities en verklaringen van afkortingen zijn opgenomen in bijlage A.1 van deze rapportage. Een overzicht van de gebruikte brondocumenten is opgenomen in bijlage A.2.

2 OPZET HAALBAARHEIDSONDERZOEK

2.1 Inleiding

Om de ontwikkelingen in de missiekritische markt goed in kaart te kunnen brengen hebben we in overleg met het ministerie van JenV ervoor gekozen om dit haalbaarheidsonderzoek op basis van een multicriteria-analyse uit te voeren. De gekozen aanpak biedt de ruimte om onzekerheden, risico's, voorkeuren, voor- en nadelen in de criteria, wegingen en de analyse tot uitdrukking te laten komen.

De behoefte aan (missie)kritische mobiele breedband communicatie binnen de Nederlandse overheid is breder dan de reikwijdte van dit onderzoek. We signaleren deze behoefte niet alleen bij het ministerie van JenV maar ook o.a. bij de ministeries van Defensie, IenW, BZK, bij overheidsorganisaties als ProRail en NS, gemeenten (gemeentelijke vervoersbedrijven, handhavingstaken, etc.), waterschappen en de mainports van Nederland, zoals o.a. Schiphol en de haven van Rotterdam. Het maakt deel uit van een brede trend in de behoefte naar meer real-time informatie.

2.2 Object van het onderzoek: Drie Scenario's

In overleg met de opdrachtgever is de keuze gemaakt om een drietal toekomstscenario's te onderzoeken. Hierbij is gezocht naar twee scenario's waarin de uitersten tot hun recht komen en een derde scenario tussen deze uitersten in. De ratio hierachter is dat het onderzoek inzicht moet geven in de *haalbaarheid* en de eigenschappen van het gebruik van op 3GPP gebaseerd mobiele breedbandtechnologie, niet in selecteren van het optimale scenario.

De huidige C2000-situatie, gebaseerd op de TETRA-oplossing van Hytera, de paging FLEX-oplossing van 2Way en daarnaast de niet-missiekritische, publieke breedbandoplossing van de drie MNO's (KPN, T-Mobile en Vodafone), zal in het onderzoek gelden als referentie en worden aangeduid met '0-scenario' of 'Huidige C2000-oplossing'. Dit 0-scenario is geen toekomst- of doelscenario en daarom in dit onderzoek niet in de uiteindelijke rangschikking van de scenario's opgenomen.

Voor het haalbaarheidsonderzoek maken we gebruik van de methode van de multicriteria-analyse. De toekomst-scenario's en het 0-scenario vergelijken we op meerdere kwalitatieve en kwantitatieve criteria. Voor elk criterium geldt dat we, waar dat mogelijk is, een zo objectief mogelijke, zoveel mogelijk op feiten gebaseerde, inschatting maken onder vermelding van de gehanteerde bronnen.

Van ieder te onderzoeken scenario zijn de voor- en nadelen in kaart gebracht op basis van de vooraf, samen met de opdrachtgever, gedefinieerde onderzoekscriteria. Het onderzoek is afgesloten met een onderbouwd advies over het te prefereren scenario. Zowel vanwege de beperkt beschikbare doorlooptijd als het verkennend karakter van het onderzoek, kent het onderzoek een beperkte diepgang.

2.3 Methodologie

De methode van multicriteria-analyse wordt toegepast bij dit onderzoek waarbij de onderzoekscriteria, inclusief sub-criteria, vooraf zijn vastgesteld in overleg met de opdrachtgever. Voor de scoringsmethodiek is een generieke 5-punten schaal het uitgangspunt per subcriterium. Deze 5-punten-schaal wordt voor kwantitatieve criteria (zoals bijvoorbeeld tijd en geld) lineair verdeeld. Voor kwalitatieve criteria (zoals bijvoorbeeld leveranciersonafhankelijk-heid) wordt op basis van argumentatie en expert opinion de mate waarin een scenario aan het betreffende (sub)-criterium voldoet, ingeschat op een percentage van 0% tot 100% met tussenliggende stappen van telkens 25%.

Doordat niet ieder hoofdcriterium een gelijk aantal subcriteria heeft is een standaardisatie (weging) toegepast waardoor ieder hoofdcriterium een resultaat scoort op een schaal van 0 tot 100. Tenslotte wordt aan elk hoofdcriterium een weegfactor meegegeven, waarmee de zwaarte waarmee een hoofdcriterium meeweegt in de totaalafweging wordt bepaald. Zodoende kunnen de toekomstscenario's onderling worden vergeleken.

Kenmerkend aan deze multicriteria analyse is dat deze voor een deel *onder onzekerheid* plaats vindt. Niet alle eigenschappen of kenmerken van de toekomstscenario's zijn immers nu al bekend. Er zal bij sommige onderdelen op basis van expert opinion een inschatting gemaakt moeten worden van de te verwachten situatie in de toekomst. Dit haalbaarheidsonderzoek is daarmee een momentopname, waarbij nu een voorkeursrichting wordt aangegeven op basis van de op dit moment beschikbare informatie.

Zo kunnen nationaalpolitieke en geopolitieke ontwikkelingen leiden tot andere prioriteiten en keuzes, kunnen ontwikkelingen in het OOV-domein leiden tot een verschuiving in de behoeftes met betrekking tot de beschikbaarheid van informatie in het veld of juist in de meldkamer en zo meer.

Om dit te ondervangen hebben wij de volgende werkwijze ingezet.

1. Allereerst geeft deze rapportage aan hoe de beoordeling tot stand is gekomen, waarbij de gehanteerde bronnen en uitgangspunten waar van belang zijn vermeld. Eventuele onzekerheden of risico's, maar ook relevante kansen worden per criterium aangegeven. Hierdoor wordt transparant op grond van welke criteria we de analyse hebben uitgevoerd en welke argumentatie we hebben gehanteerd bij de beoordeling. Tevens vullen we daarmee de behoefte in om de risico's vooraf te identificeren en, waar mogelijk, de maatregelen te bepalen om deze te beheersen.
2. Om de toekomstige veranderingen te kunnen meenemen in een latere herijking van de uitkomst van dit haalbaarheidsonderzoek hebben wij, op basis van onze eigen (uiteraard beargumenteerde) expert opinion, aangegeven welke weging elk criterium in onze ogen verdient. Deze wegingsfactoren en beoordelingen zijn voorgelegd aan de begeleidingsgroep voor een second opinion. Bij een afwijkend oordeel is dit bediscussieerd en is onderzocht of er, gelet op de gedane aannames of aangedragen feiten en/of argumenten, een aanpassing van de weging moet komen. Bij een latere herijking van de uitkomsten van dit onderzoek kan relatief eenvoudig worden bepaald of de veranderde omstandigheden van invloed moeten zijn op de criteria, hun weging en de beoordeling van de scenario's en zo ja, in welke mate.

De aanpak van het onderzoek bestaat uit de volgende stappen:

- Bepalen van de toekomstscenario's
- Opstellen van de criteria en de scoremethodiek
- Bepalen van de weging van de (sub)criteria
- Uitvoeren van de evaluatie
- Bepalen van de rangorde van de toekomstscenario's

Deze stappen zijn in de volgende paragrafen nader uitgewerkt. In elke stap leggen we de wijze waarop de validatie plaatsvindt vast.

2.4 Scenario's haalbaarheidsonderzoek

2.4.1 Inleiding

Voordat we de gekozen scenario's toelichten is het van belang inzicht te geven in de wijze waarop mobiele communicatienetwerken zijn opgebouwd. Mobiele communicatienetwerken bestaan op hoofdlijnen uit een

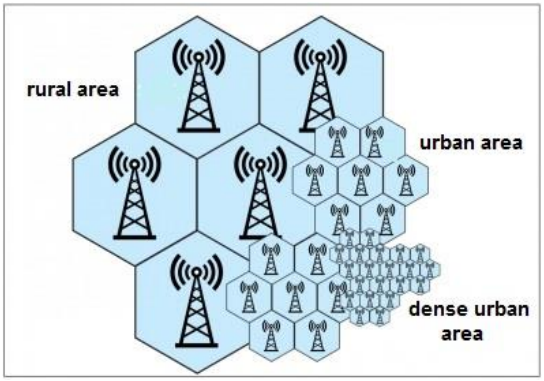
radionetwerk, een transmissienetwerk en een core-netwerk. Voor de realisatie van een mobiel communicatie-netwerk wordt de 3GPP-technologie en architectuur toegepast in de netwerkcomponenten. Voor een netwerk wordt een ontwerp gemaakt met netwerkcomponenten op basis van de eisen die aan het netwerk gesteld worden. Voor deze componenten zijn meerdere leveranciers op de markt die geselecteerd kunnen worden op basis van onder andere technische, financiële en veiligheidscriteria. Nadat het netwerk gerealiseerd is zal dit beheerd moeten worden door een beheerorganisatie. Het is mogelijk om de componenten als eigenaar van het netwerk zelf aan te schaffen en te beheren. Het is aan de andere kant ook mogelijk om netwerkfunctionaliteit inclusief beheer als dienst van een dienstenleverancier in te kopen. Deze dienstenleverancier is dan eigenaar en beheerder van de netwerk-componenten.

2.4.1.1 Radionetwerk

Het radionetwerk bestaat uit **opstelpunten** (masten met antennes) en vormt de eerste (deels draadloze) verbinding tussen de randapparaten in het veld, zoals de portofoons, camera's, smartphones, tablets en dergelijke, en het overige deel van het mobiele netwerk. Het radionetwerk is zo ontworpen dat de opstelpunten in een specifiek gebied voldoende **radiodekking** realiseren. Radiodekking is het eerste vereiste om een mobiel netwerk te laten functioneren. Voor radiodekking is **frequentie**spectrum nodig. De frequenties voor 3GPP gebaseerde mobiele breedbandnetwerken zijn wereldwijd gestandaardiseerd en vormen een zeer schaars goed. Het frequentiespectrum wordt in Nederland beheerd en uitgegeven door het ministerie van EZK. De mast met antennes en de benodigde actieve apparatuur (die een stroomvoorziening vereist) van het Radionetwerk wordt **basisstation** genoemd. Het specifieke deel waar een basisstation radiodekking voor creëert, wordt ook wel **radiocel** genoemd. Het aantal benodigde antenne-opstelpunten is in principe afhankelijk van de volgende factoren:

- De gebruikte radiofrequentie. Een belangrijke eigenschap van een specifieke frequentie is de reikwijdte ervan. Hoe hoger de frequentie, hoe kleiner de reikwijdte en hoe kleiner de cellen zijn. Om grotere gebieden van dekking te voorzien, zijn dan meer antenne-opstelpunten nodig.
- De bebouwing en terreinkarakteristieken (zoals bijvoorbeeld heuvels, bos, water) in het gebied. Meer bebouwing betekent dat het radiosignaal wordt gereflecteerd en gedempt. Lagere frequenties ondervinden minder last van demping dan hogere frequenties. Om in een gebied met veel bebouwing toch een sterk radiosignaal te realiseren zijn meer antenne-opstelpunten nodig. Voor radiodekking binnenshuis geldt ook dat lagere frequenties (kleiner dan 1 GHz) minder verstoord worden door bebouwing.
- De minimale signaalsterkte. Er is een minimale signaalsterkte nodig voor een kwalitatief goede verbinding. De afstand tussen de antennelocaties zal zo gekozen worden, dat overal een optimale signaalsterkte kan worden gerealiseerd.
- De benodigde netwerkcapaciteit. Door meer frequentiespectrum in te zetten kan de capaciteit van het netwerk vergroot worden. In de hogere frequenties is meer spectrum beschikbaar. Hogere frequenties hebben echter minder bereik. Als een hoge capaciteit gewenst is, zijn in veel gevallen meer antenne-opstelpunten nodig.

Voorbeeld: Voor mobiele netwerken die functioneren met een frequentie in de 700-900MHz band zijn minder antenne-opstelpunten nodig om een gebied van radiodekking te voorzien dan netwerken die met frequenties in de 2000MHz of 3500MHz band werken. In onderstaand figuur is weergegeven de wijze waarop een radionetwerk, voor het realiseren van radiodekking, kan zijn opgebouwd uit een mix van grote en kleine radiocellen. Voor landelijke omgeving met weinig bebouwing en capaciteitsbehoefte kunnen lagere frequenties met grotere radiocellen worden gebruikt. Voor de dichtbevolkte stedelijke gebieden, worden kleine radiocellen gebruikt met een grote capaciteit.



Figuur 1. Opbouw mobiel radionetwerk

2.4.1.2 Transmissienetwerk

Het transmissienetwerk zorgt voor het transport van data tussen de antenne-opstelpunten en het core-netwerk. De data die getransporteerd wordt is uiteraard de communicatie tussen gebruikers maar ook de signaleringsdata, die noodzakelijk is voor het goed functioneren van het gehele netwerk. Het transmissienetwerk verbindt alle basisstations met de core. Fysiek bestaat het transmissienetwerk uit draadloze straalverbindingen of fysieke kabels (zoals nu veelal via glasvezel of nog via koperkabel). Het transmissienetwerk maakt gebruik van actieve apparatuur, welke een eigen stroomvoorziening vereisen. Bij het ontwerp van het transmissienetwerk is het mogelijk om de beschikbaarheid te verhogen door basisstations via meerdere gescheiden routeringen in het transmissienetwerk te verbinden, onderling en met het core-netwerk. Of dit ook daadwerkelijk gebeurt, is afhankelijk van de ontwerp-criteria van een netwerk. Voor een missiekritisch netwerk kan dit een harde eis zijn, voor een commercieel mobiel netwerk van een mobiele operator kunnen andere uitgangspunten het ontwerp bepalen.

Door de vele verbindingen en eventueel benodigd graafwerk om de verbindingen aan te leggen maakt het transmissienetwerk relatief een groot deel uit van de totale investering van een mobiel netwerk. Voor meer detail verwijzen we naar hoofdstuk 5 waarin de financiële vergelijking van de scenario's op hoofdlijnen is gemaakt. In het dichtbebouwde Nederland is een wijdvertakt netwerk van vooral glasvezelverbindingen en straalverbindingen beschikbaar en zijn vele marktpartijen actief die transmissiediensten aanbieden. Hierdoor is er veelal geen noodzaak om het landelijke transmissienetwerk volledig in eigen beheer aan te leggen en kunnen zo de aanlegkosten aanzienlijk worden verlaagd.

2.4.1.3 Core-netwerk

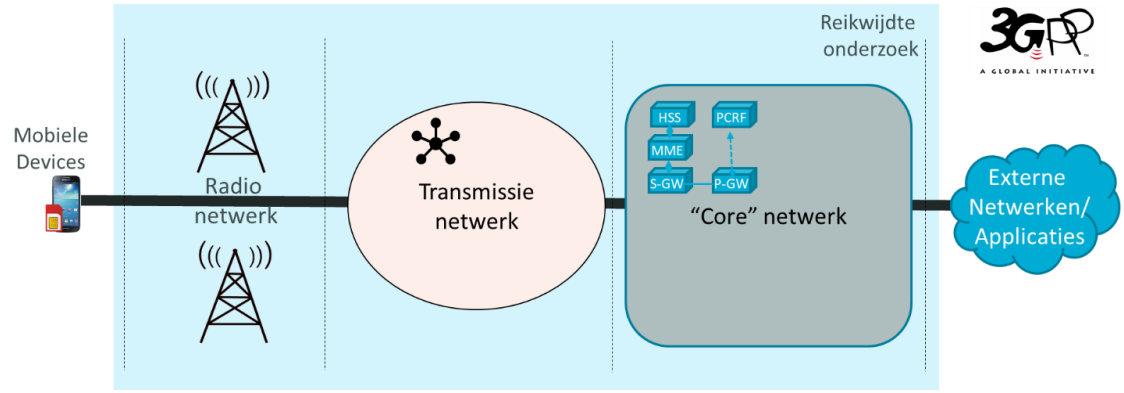
Het core-netwerk (hierna: de core) is het centrale deel van een mobiel netwerk. De core zorgt voor de routering van gesprekken en datastromen, de (gebruikers)administratie, gebruikersrechten, samenstelling van mobiele diensten, security en eventuele billing. Het core-netwerk bevat 3GPP-gestandaardiseerde componenten zoals:

- HSS (Home Subscriber Server) waarin de gebruikers van het mobiele netwerk geregistreerd worden;
- MME (Mobility Management Entity) verantwoordelijk voor de authenticatie van een gebruiker;
- S-GW (Serving Gateway) voor de routering van gebruikers data;
- P-GW (Packet Gateway) verbindt het mobiele netwerk met externe netwerken zoals bijvoorbeeld het eigen datanetwerk of het internet;

- PCRF (Policy and Charging Rules Function) bepaalt real time de mobiele netwerkfuncties van een gebruiker. Via de core vindt ook uitwisseling plaats met eventuele andere netwerken of toepassingen/applicaties (bijvoorbeeld via een zogenoemd IP Multimedia Subsystem, IMS-platform).

De core staat opgesteld in een datacenter omgeving en is veelal meervoudig uitgevoerd op verschillende locaties om zo een hoge beschikbaarheid van het totale mobiele netwerk te borgen.

Schematisch is de opbouw van een mobiel breedbandnetwerk weergegeven in de volgende afbeelding. In deze afbeelding geeft de rechthoek de reikwijdte van het onderzoek aan. Het onderzoek beperkt zich tot het mobiele breedbandnetwerk. De mobiele devices, de externe netwerken en (MCX) applicaties vallen erbuiten. Dit mobiele breedbandnetwerk vormt de verbinding, zogenaamde connectiviteit, tussen het mobiele device en de externe netwerken en toepassingen/applicaties.



Figuur 2. Schematische opbouw mobiel breedbandnetwerk

2.4.2 Toekomstscenario's

Voor elk van de drie genoemde netwerkdelen zijn twee essentiële keuzes relevant:

1. Wie is de eigenaar van het netwerk, de overheid zelf of is dat een leverancier?
2. Wie beheert het netwerk, de overheid zelf of voert een leverancier het beheer uit voor de overheid?

Theoretisch kunnen deze keuzes los van elkaar en voor elk netwerkonderdeel weer los gemaakt worden, wat neerkomt op een totaal van 64 (4x4x4=64) mogelijke varianten. In de praktijk blijkt het aantal voorkomende situaties drastisch lager.

In overleg met de opdrachtgever is de keuze gemaakt om een 3-tal toekomstscenario's te onderzoeken. Hierbij is gezocht naar twee scenario's waarin de uitersten tot hun recht komen en een derde scenario tussen de uitersten in. De ratio hierachter is dat het onderzoek inzicht moet geven in de *haalbaarheid* van het gebruik van mobiele breedband technologie, niet in de exacte specificaties van het optimale scenario.

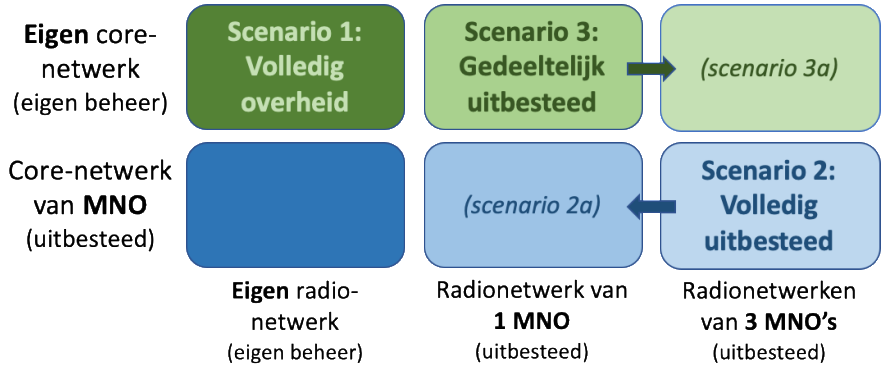
Het uitlichten van de uitersten geeft inzicht in de eigenschappen, consequenties en risico's van de verschillende scenario's en geeft zicht op aanvullende keuzen en maatregelen die genomen moet worden om ongewenste effecten te voorkomen dan wel te verminderen.

De enige uitzondering is het transmissienetwerk dat in alle gevallen als dienst van marktpartijen wordt afgenomen. Hiervoor is gekozen omdat het transmissienetwerk aanzienlijk efficiënter (tegen aanzienlijk lagere kosten) logisch zo

ingericht (en ingekocht) kan worden dat de overheid alsnog vrijwel de volledige controle heeft. Dit om te voorkomen dat dit scenario op voorhand al financieel onaantrekkelijk is.

Weliswaar gaat het in dit onderzoek om de haalbaarheid van mobiele breedband technologie voor missiekritische toepassingen, maar omdat de keuze reeds gemaakt is voor op 3GPP standaarden gebaseerde technologie, zijn de vraagstukken die betrekking hebben op eigenaarschap, zeggenschap, veiligheid, organisatie en politieke aspecten meer onderscheidend.

Om die reden is ervoor gekozen om drie scenario's te formuleren waarin deze niet-technologische vraagstukken het beste tot uitdrukking komen. Naast deze drie scenario's, hebben we twee varianten in ogenschouw genomen. Deze scenario's 2a en 3a zijn niet in de multicriteria analyse als zelfstandige scenario's onderzocht. We hebben van deze varianten alleen de financiële verschillen ten opzichte van de scenario's 2 en 3 in kaart gebracht om zo meer inzicht te geven in de financiële consequenties van de verschillende keuzes. De scenario's en varianten zijn schematisch weergegeven in de navolgende figuur 3.



Figuur 3. Schematische weergave onderzoekscenario's

1. **Volledig overheid**: De overheid heeft het volledige mobiele breedband netwerk voor missiekritische communicatie aangeschaft (in eigendom verkregen) en voert zelf het beheer over dit netwerk. De enige uitzondering is, zoals eerder aangegeven, het transmissienetwerk dat als dienst van marktpartijen wordt afgenomen.
   Voor de volledigheid, de overheid ontwikkelt in dit scenario niet haar eigen technologie, netwerk of randapparatuur, dit wordt van marktpartijen afgenomen. Alle mobiele toepassingen (inclusief paging) worden afgewikkeld in het mobiele breedband netwerk.

Invulling Scenario 1

Radionetwerk		Transmissienetwerk		Core netwerk	
Eigenaarschap	Beheer	Eigenaarschap	Beheer	Eigenaarschap	Beheer
In eigendom	Zelf doen	In eigendom	Zelf doen	In eigendom	Zelf doen
Uitbesteed	Uitbesteed	Uitbesteed	Uitbesteed	Uitbesteed	Uitbesteed

2. **Volledig uitbesteed**: De overheid neemt het mobiele breedband netwerk als dienst af van MNO's op basis van nader af te spreken tarieven en dienstniveau. In dit scenario is de variant gekozen om de dienst niet van één maar van alle Nederlandse mobiele netwerk operators af te nemen. De radionetwerken van de drie MNO's worden in dit scenario ingezet om de radiodekking en de beschikbaarheid van de dienst te verhogen.

Kenmerkend aan dit scenario is dat de mobiele breedband netwerken eigendom zijn van de betreffende operators en ook volledig door de operators, of onder hun regie, worden beheerd. Alle mobiele toepassingen (inclusief paging) worden afgewikkeld via de mobiele breedband dienst.

Invulling Scenario 2

Radionetwerk		Transmissienetwerk		Core netwerk	
Eigenaarschap	**Beheer**	**Eigenaarschap**	**Beheer**	**Eigenaarschap**	**Beheer**
In eigendom	Zelf doen	In eigendom	Zelf doen	In eigendom	Zelf doen
Uitbesteed	Uitbesteed	Uitbesteed	Uitbesteed	Uitbesteed	Uitbesteed

3. **Gedeeltelijk uitbesteed:** De overheid heeft in dit scenario het core-netwerk in eigendom (en beheer) en het radionetwerk is uitbesteed aan één mobiele operator op basis van nader af te spreken tarieven en dienstniveau. In dit scenario is de variant gekozen om het radionetwerk van één mobiele operator af te nemen om onderscheid te maken met scenario 1 waarbij de overheid zowel en core- als radionetwerk in eigendom heeft en met scenario 2 waarbij er geen redundantie is van het radionetwerk van meerdere MNO's.

Invulling Scenario 3

Radionetwerk		Transmissienetwerk		Core netwerk	
Eigenaarschap	**Beheer**	**Eigenaarschap**	**Beheer**	**Eigenaarschap**	**Beheer**
In eigendom	Zelf doen	In eigendom	Zelf doen	In eigendom	Zelf doen
Uitbesteed	Uitbesteed	Uitbesteed	Uitbesteed	Uitbesteed	Uitbesteed

In deze toekomstscenario's verstaan we onder 'overheid' een publiekrechtelijke rechtspersoon waar de besturing-, ontwerp- en beheerfuncties onder eigen directe aansturing worden uitgevoerd.

De scenario's zien op de periode 2025 tot 2035.

Een hybride scenario waarin meerdere technieken tegelijkertijd worden ingezet (bijvoorbeeld TETRA-technologie voor spraak en een 4G-netwerk voor breedbanddata) is ook overwogen. Hoewel er partijen in de markt zijn die hierover een andere opvatting hebben, zijn wij van mening dat de TETRA-technologie als missiekritische hoofdoplossing voor een Europese overheid ruim voor 2035 niet meer toegepast zal worden, de toepassing zal op termijn hooguit als "last resort fall back" voorziening nog ingezet worden. Om die reden is dit scenario voor ons een tijdelijke migratie (**M**) situatie waarbij de huidige situatie, mogelijk geleidelijk, wordt omgezet naar de nieuwe, mobiele breedbandoplossing. Deze hybride oplossing is daarmee geen doelscenario en om die reden niet separaat onderzocht.

De huidige situatie met C2000 en publieke (niet missiekritische) mobiele breedband diensten geldt in het onderzoek als referentie en wordt aangeduid als het 0-scenario of de Huidige C2000-oplossing (**0**). Ook dit is eveneens geen toekomst- of doelscenario.

2.5 Criteria en scoremethodiek

Op basis van onze expert opinion hebben we een eerste keuze gemaakt van de relevante criteria en deze met de begeleidingsgroep besproken en bijgesteld. Gelet op de onzekerheden die er zijn over de exacte invulling van de toekomstscenario's is het niet doenlijk om een uitputtende vergelijking te maken van alle functionaliteiten, dekking, spraakkwaliteit, koppelvlakken etc. met eenzelfde detailniveau zoals dat gehanteerd zou worden in een selectiefase van een aanbesteding van een missiekritisch systeem.

In onderling overleg met de opdrachtgever hebben we de te onderzoeken criteria voor de vergelijking van de scenario's vastgesteld. Hierbij is onderscheid gemaakt naar dertien hoofdcriteria met per criterium één of meerdere subcriteria. Dit resulteert in een totaal van 51 subcriteria.

In onderstaande tabel zijn de 13 hoofdcriteria met de subcriteria opgenomen. In bijlage A3 van dit rapport is de uitgebreide omschrijving per subcriterium opgenomen.

Criterium	Subcriterium
1. Strategisch/ politiek	1.1: Mate van zeggenschap om nationale economische, politieke en/of veiligheidsbelangen te kunnen borgen (sturing)
	1.2: Mate van onafhankelijkheid van leveranciers
	1.3: Passend in internationale politieke samenwerkingen
	1.4: Mate van zeggenschap om een zekere (minimale) operationele beschikbaarheid bij calamiteiten/rampen te kunnen borgen.
2. Techniek	2.1: Functionele beschikbaarheid
	2.2: Technische beschikbaarheid
	2.3: Buitenhuisdekking
	2.4: Binnenhuisdekking
	2.5: Capaciteit
	2.6: Fallback
	2.7: Functionaliteit
	2.8: Open standaarden
	2.9: Interoperabiliteit/ koppelvlakken
	2.10: Alarmering (Paging)
	2.11: Volwassenheid van oplossing (proven technology)
3. Beveiliging	3.1: Beveiliging van het gehele systeem
	3.2: Exclusiviteit – access control, authenticatie
	3.3: Vertrouwelijkheid – vercijfering
	3.4: Integriteit – weerbaarheid tegen manipulatie

	3.5: Monitoring/logging
4. Innovatie en toekomstvastheid	4.1: De mate waarin de oplossing wordt doorontwikkeld als ook de levensduur van de oplossing.
	4.2: De mate waarin de oplossing de doorontwikkeling van diensten en aanvullende functionaliteit faciliteert en/of ondersteunt.
5. Frequentie spectrum	5.1: Spectrum efficiëntie
	5.2: Capaciteit
6. Organisatie	6.1: Projectorganisatie (verwerving systeem)
	6.2: Benodigde (beheer)organisatie (exploitatie)
7. Financieel	7.1: Financiële vergelijking
8. Besturing	Bestuurlijke inrichting en de rolverdeling tussen opdrachtgever en opdrachtnemer. Voor- en nadelen per oplossing t.a.v. de bestuurlijke inrichting, inclusief de afweging om (onderdelen) zelf te doen dan wel uit te besteden. 8.1: Functionele en technische inrichting
	8.2: Operationeel beheer
	8.3: Toekomstige verbeteringen
	De mate waarin juridische aspecten van toepassing zijn op de oplossing en welke. Juridisch mogelijk relevante onderdelen zijn:
9. Juridisch	9.1: Beschikbaarheid spectrum/ veiling
	9.2: Privacy aspecten
	9.3: Bewijsgaring, bewijsvoering
	9.4: Mededingingswetgeving
	9.5: Aanbestedingswetgeving
	9.6: Telecomwetgeving (incl. netneutraliteit)
	De mate waarin verwacht mag worden dat de oplossing in 2025 beschikbaar is en van 2025-2035 gebruikt kan worden. Bij dit criterium komt een aantal aspecten naar voren:
10. Tijd / planning	10.1: Releaseplanning 3GPP, en de tijd om het systeem te ontwikkelen, testen en operationeel te maken

	10.2: Tijd voor verwerving/aanbesteding (4 – 6 jaar)
	10.3: Tijdpaden wanneer een oplossing beschikbaar is
	10.4: Afhankelijkheden van andere ontwikkelingen: (Veiling 5G, GSM-R en ERTMS, Schiphol aanbesteding, smart meter, et cetera.
	10.5: Ontwikkeling van 4G/LTE naar 5G en mogelijke opvolgers.
	10.6: Hoe lang kan nog worden gewerkt met 4G, TETRA, FLEX ™ et cetera?
11. Internationaal	11.1: De mate waarin internationale ontwikkelingen kunnen bijdragen aan en/of worden opgenomen in de oplossing.
	11.2: 3GPP-standaarden
	11.3: Mate van mogelijke operationele afstemming met de omringende landen
	11.4: Grensoverschrijdende dekking (roaming)
	Mate waarin vanuit de huidige situatie de gewenste doelsituatie zonder onderbreking en met minimale belasting van de eindgebruikers kan worden bereikt. Aspecten die hierbij een rol spelen zijn:
12. Migratie	12.1: Mogelijkheid om onafhankelijk van de huidige oplossing te migreren
	12.2: Eenvoud van migratie.
	12.3: Storingsvrije migratie.
	Criterium overstijgende kansen/risico's zijn opgenomen binnen de categorie Risico's. Voor zover kansen en risico's direct bij een criterium horen, worden die bij dat betreffende criterium opgenomen.
13. Risico's	13.1: Risico's van de oplossing (functioneel/techniek, tijdslijnen, kosten, organisatie, juridisch).
	13.2: Kansen vanuit de oplossing die kunnen bijdragen aan verbeteringen.

Elk van de drie scenario's is op elk subcriterium beoordeeld. Hierbij is in principe een 5-puntenschaal gebruikt waarbij in discrete stappen van 25% aangegeven is, in hoeverre het betreffende toekomstscenario voldoet aan het betreffende subcriterium. In de onderstaande tabel is de classificatie en puntenwaardering weergegeven.

Classificatie per subcriterium	Afgekort	Punten
Volledig in te vullen in scenario	Volledig	100
Grotendeels in te vullen met maatregelen	Grotendeels	75
Deels in te vullen met maatregelen	Deels	50
Beperkt haalbaar	Beperkt	25
Niet in te vullen in scenario	Niet	0

Bij enkele kwantitatieve criteria, zoals bijvoorbeeld tijd, is geen discrete verdeling in vijf stappen gebruikt, maar is een lineaire verdeling toegepast.

2.6 Weging van de (sub)criteria

Bij elk criterium en bij elk subcriterium hebben we vanuit onze expert opinion een weging aangebracht, dat aangeeft hoe zwaar elk (sub)criterium meeweegt. Deze is met de opdrachtgever besproken, waarna de definitieve weging is vastgesteld. De weging van de subcriteria binnen een hoofdcriterium is zodanig dat die optellen tot 100%. De hoofdcriteria hebben een waarde gekregen die varieert van minimaal 1 tot maximaal 3. Het overzicht van alle weegfactoren is opgenomen in bijlage A5. Bij de weging zijn we uitgegaan van het belang voor de operatie. Aangezien het gaat om missiekritische communicatie, dat wil zeggen dat er mensenlevens op het spel kunnen staan, hebben we de criteria die bepalend zijn voor de betrouwbare, operationele werking van de oplossing het hoogst gewaardeerd. Het overzicht van alle weegfactoren is opgenomen in het Excel-bestand (*Bijlage 1 Haalbaarheidsonderzoek missiekritische communicatie - Kwalitatieve criteria beoordeling v1.0.xlsx*) dat als losse bijlage bij dit rapport hoort.

2.7 Uitvoering evaluatie

De volgende stap in de aanpak is de evaluatie van elk van de drie toekomstscenario's tegen de vastgestelde criteria. Van elke score is steeds de gehanteerde argumentatie vastgelegd. Het is niet mogelijk om voor alle criteria de toekomstscenario's te vergelijken met de huidige C2000-invulling. Bijvoorbeeld op het punt van radiodekking hangt het er maar vanaf hoeveel antenne-opstelpunten straks in een toekomstscenario worden geplaatst. Waar een score niet mogelijk is of waar het afhangt van nadere operationele of financiële keuzes geven we dat aan en beschrijven we dat in termen van risico's. Ook in die gevallen dat op een criterium geen verschil is tussen de scenario's beschrijven we dit, omdat ook het gegeven dat een criterium niet leidt tot differentiatie tussen de scenario's nog steeds relevant is.

2.8 Bepalen van rangorde toekomstscenario's

De beoordeling van alle subcriteria heeft geleid tot een score per subcriterium. De scores van de subcriteria zijn geconsolideerd per hoofdcriterium. Door vervolgens de weegfactoren per hoofdcriterium toe te passen, is de uitkomst van de vergelijking van de toekomstscenario's tot stand gekomen. Het resultaat is een rangorde van de drie toekomstscenario's, die de basis vormt voor het advies voor het voorkeursalternatief. De beoordeling is besproken met de opdrachtgever om de onzekerheden, gemaakte inschattingen en uitkomst van de scores en de juistheid van de weging te valideren.

3 HUIDIGE SITUATIE EN ONTWIKKELINGEN

3.1 Inleiding

In dit hoofdstuk geven we een inzicht in de huidige situatie op het gebied van missiekritische netwerken in Nederland, Europa en daarbuiten. Verder belichten we de stand van zaken ten aanzien van de mobiele breedband technologie-ontwikkelingen en de stand van zaken van landen en overheden die reeds een keuze hebben gemaakt voor de toekomstige missiekritische mobiele communicatieoplossing voor de openbare orde en veiligheidsorganisaties.

3.2 Huidige situatie in Nederland

In Nederland kennen we C2000. C2000, de naam die gegeven is aan een communicatievoorziening die in 2004 volledig operationeel is geworden, bestaat uit twee onderdelen:

- P2000, het alarmeringsnetwerk dat met name door veel veiligheidsregio's wordt gebruikt voor het uitzenden van alarmeringsberichten;
- T2000, het op TETRA-technologie gebaseerde portofoon netwerk. Dit wordt gebruikt voor spraakcommunicatie, door middel van groepsoproepen en individuele oproepen, en voor het versturen van korte databerichten.

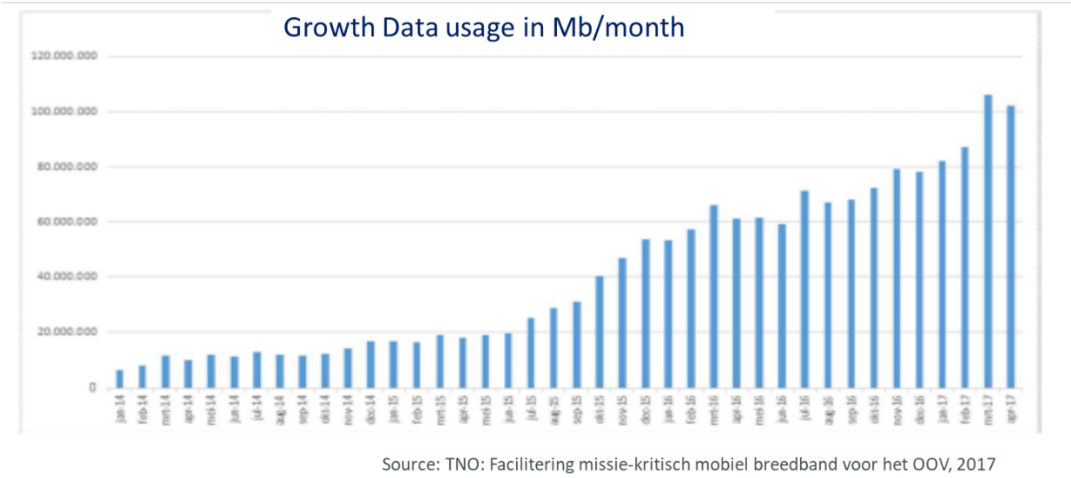
In januari 2020 is het nieuwe C2000-netwerk operationeel geworden. Het oude netwerk was aan het einde van de levensduur. Zowel het P2000- als het T2000-netwerk zijn vervangen. De randapparatuur is hierbij niet vervangen. De randapparatuur heeft een kortere levensduur dan het netwerk en is tussentijds al één of meerdere malen vervangen. Zowel de netwerken als de randapparatuur van C2000 zijn in eigendom bij de Nederlandse overheid. Het C2000-netwerk maakt gebruik van frequentiespectrum dat door het ministerie van EZK is toegewezen, via een licentie aan het ministerie van JenV. De aangewezen gebruikers van C2000 zijn de politie, de veiligheidsregio's, de ambulancediensten en het ministerie van Defensie. Daarnaast zijn er tientallen gelieerde gebruikers, zoals reddingsbrigades, waterschappen, Rijkswaterstaat, Douane, DJI, opsporingsdiensten en industriële concerns en energiebedrijven.

Het netwerk bestaat uit een core-netwerk en ruim 600 base stations/antenne-opstelpunten waarmee de radiodekking 'buiten' over geheel Nederland wordt verzorgd. De overheid heeft diverse locaties aangewezen (de zogenoemde special coverage locations, ook wel SCL's genoemd), waarvan de objecteigenaren voor eigen kosten binnenhuis radiodekking van het TETRA-netwerk van C2000 moeten voorzien. Voorbeelden van SCL's zijn stadions, tunnels, ziekenhuizen, en luchthavens.

De opdracht tot vernieuwing van C2000 is in 2015 gegund aan een combinatie van drie bedrijven, waaronder een dochter van het Chinese bedrijf Hytera. Naar aanleiding van toegenomen zorgen over de groeiende invloed van statelijke actoren en veranderende geopolitieke verhoudingen zijn verschillende onderzoeken uitgevoerd naar de veiligheid van C2000, onder andere door de AIVD. In haar onderzoeksrapport adviseerde de AIVD om over te gaan naar een oplossing waarbij de afhankelijkheid van landen met een offensief cyberprogramma gericht tegen Nederlandse belangen is geminimaliseerd.

Naast het gebruik van C2000 maken de openbare orde en veiligheidsdiensten (OOV-organisaties) op dit moment ook gebruik van de standaard mobiele breedbanddiensten van de Nederlandse mobiele operators. Deze diensten zijn standaard 4G-diensten van de operators met een "best effort" serviceniveau en dus niet specifiek missiekritisch ingericht. Met deze dienstverlening wordt nu een deel van de mobiele breedband behoefte van de OOV-organisaties in Nederland ingevuld. Het belang voor de uitvoering van de operationele taken van de OOV-organisaties neemt toe, waarbij de toepassingen van "nice to have" zijn verschoven naar "need to have". In onderstaande figuur is de

ontwikkeling van het mobiel breedband verkeer bij de Nederlandse politie in de periode 2014 tot 2017 afgebeeld. Deze ontwikkeling laat een groei zien die vergelijkbaar is met het gebruik van data door consumenten en bedrijven.



Source: TNO: Facilitering missie-kritisch mobiel breedband voor het OOV, 2017

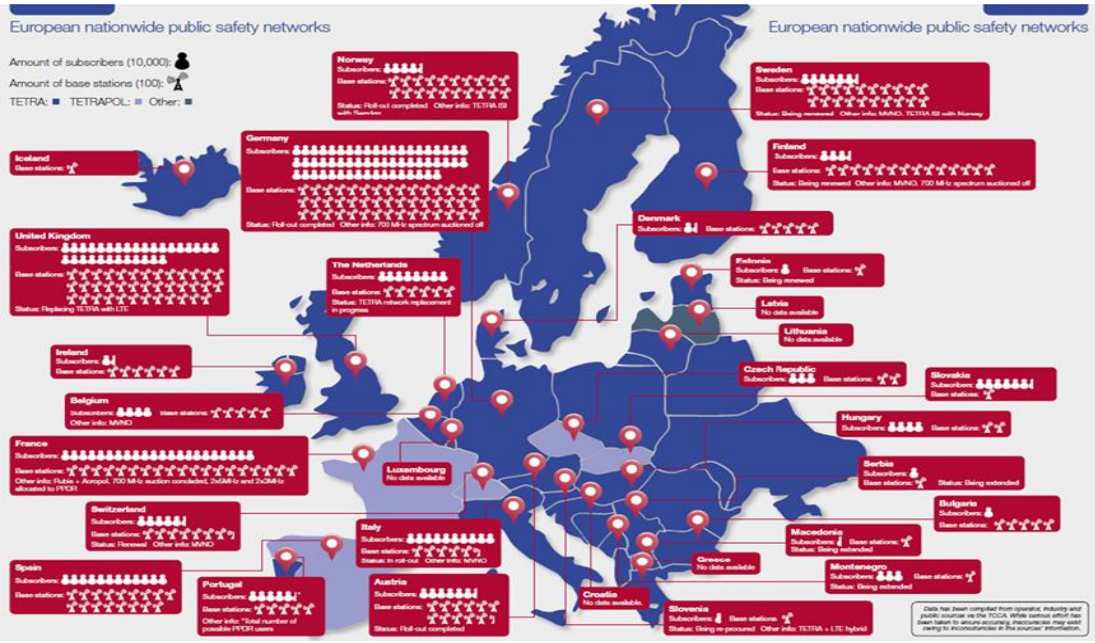
Figuur 4. Groei van mobiel breedband verkeer bij Politie NL, bron TNO

In Nederland zijn op dit moment drie mobiele netwerk operators actief die allen mobiele breedband diensten in concurrentie aanbieden aan de markt. De drie mobiele netwerken worden elk jaar getest op kwaliteit door de onafhankelijke testorganisatie P3. Eén van de terugkerende conclusies van deze testen is dat Nederland drie kwalitatief goede, openbare mobiele breedbandnetwerken heeft.

3.3 Huidige situatie in Europa

Binnen Europa heeft op dit moment ieder land een eigen oplossing voor missiekritische communicatie. In de navolgende figuur is een overzicht weergegeven van de huidige Europese 'public safety'-netwerken. Er zijn twee technologieën in gebruik, beide gebaseerd op smalbandige communicatie; lichtpaars gekleurde landen gebruiken TETRAPOL als technologie, de donkerpaars gekleurde landen gebruiken netwerken gebaseerd op TETRA-technologie. In de roodgekleurde vlakken is per land het aantal base stations weergegeven waarbij elke antenne 100 basestations vertegenwoordigt. Het aantal poppetjes geeft het aantal gebruikers of abonnementen/mobiele devices (maal 10.000) weer. In totaal zijn er binnen Europa in de diverse missiekritische smalbandnetwerken 23.000 base stations en 2,1 miljoen mobiele devices. 80% van de netwerken maakt gebruik van de TETRA-technologie en 20% gebruikt TETRAPOL. Het grootste TETRA-netwerk in de wereld is geïmplementeerd in Duitsland door BDBOS. Qua omvang is Nederland met ruim 600 base stations en ongeveer 100.000 devices een kleine speler.

TETRA is een Europese ETSI (European Telecommunications Standards Institute) standaard. TETRAPOL is een proprietary standaard; het is gebaseerd op de technologie van één leverancier. TETRA en TETRAPOL zijn gebaseerd op digitale communicatietechnologie uit de jaren 90 van de vorige eeuw.



Figuur 5. Overzicht van public safety netwerken in Europa, bron: TCCA, www.tcca.info

3.4 Huidige situatie in de rest van de wereld

In de Verenigde Staten was van oudsher geen landelijk dekkend missiekritisch netwerk beschikbaar, maar werden deze netwerken per stad, regio of staat gerealiseerd. Veelal zijn deze netwerken op basis van de P25 of APCO-25 standaard gebouwd. P25 kan gezien worden als de Amerikaanse tegenhanger van TETRA. In de jaren na de aanslag van 9 september 2001 werd de behoefte om staat overschrijdend te communiceren manifest en is het FirstNet-initiatief gestart vanuit de federale overheid. Zie hiervoor paragraaf 3.9.2.

In andere landen, buiten de VS en Europa, zijn public safety netwerken gebouwd op basis van de Europese TETRA-standaard en op basis van de Amerikaanse P25-standaard. Daarnaast worden er in veel landen, buiten Europa en de VS, nog oplossingen gebruikt op basis van verouderde, analoge mobiele communicatietechnologie.

3.5 Ontwikkelingen in de technologie

De standaarden TETRA en TETRAPOL worden al geruime tijd niet meer verder ontwikkeld. Tot 7 à 10 jaar geleden lag de toekomst voor missiekritische public safety netwerken nog op de smalbandige TETRA-technologie met de TETRA-2 standaard, waarin ook de datatoepassingen destijds voorzien waren met TEDS (TETRA Enhanced Data Services).

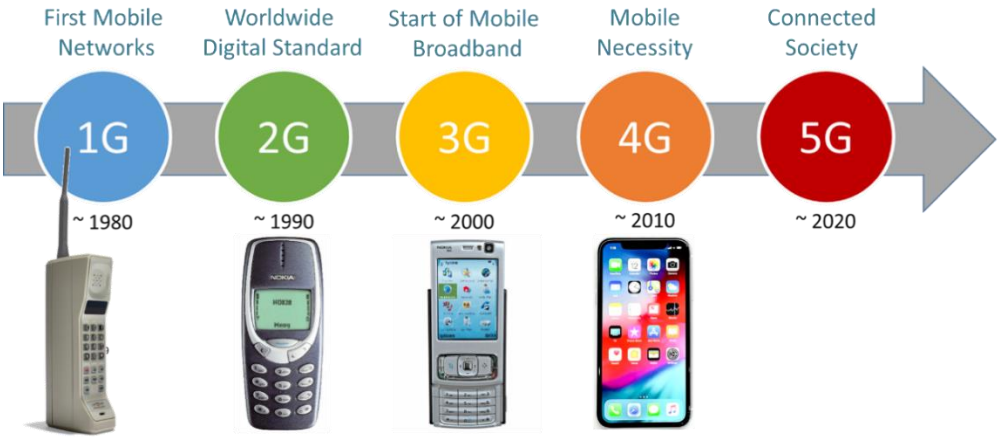
Inmiddels evolueert de behoefte van missiekritische gebruikers sterk naar breedbandige oplossingen. De ontwikkeling naar de toekomst vindt plaats in de technologie die is gebaseerd op de 3GPP-standaarden. Verschillende overheden in de wereld hebben al een principe keuze gemaakt door de toekomst van missiekritische communicatie te baseren op de open 3GPP-standaarden. Dit komt nader aan de orde in paragraaf 3.8 en verder.

De ontwikkeling van mobiele communicatietechnologie vindt op wereldniveau plaats binnen de 3GPP (3rd Generation Partnership Projects) standaardisatie organisatie. De 3GPP verenigt 7 telecommunicatie standaardisatie-organisaties en draagt zorg voor de standaardisatie van mobiele communicatietechnologie en netwerken. De deelnemers hebben verschillende achtergronden, te denken valt aan netwerktechnologie leveranciers, chipmakers voor

mobiele randapparatuur, vertegenwoordigers van gebruikers, operators en research organisaties. De doelstelling van de standaarden is het creëren van een leveranciersonafhankelijk, open ecosysteem van oplossingen voor mobiele netwerkcomponenten en mobiele randapparatuur waarbij de samenwerking is gewaarborgd.

De standaarden worden overal ter wereld toegepast in de huidige, publieke, mobiele netwerken door MNO's. Deze MNO's bieden publieke, mobiele communicatiediensten aan de massamarkten. Op dit moment zijn er meer dan 8 miljard mobiele randapparaten verbonden met op 3GPP gebaseerde netwerken.

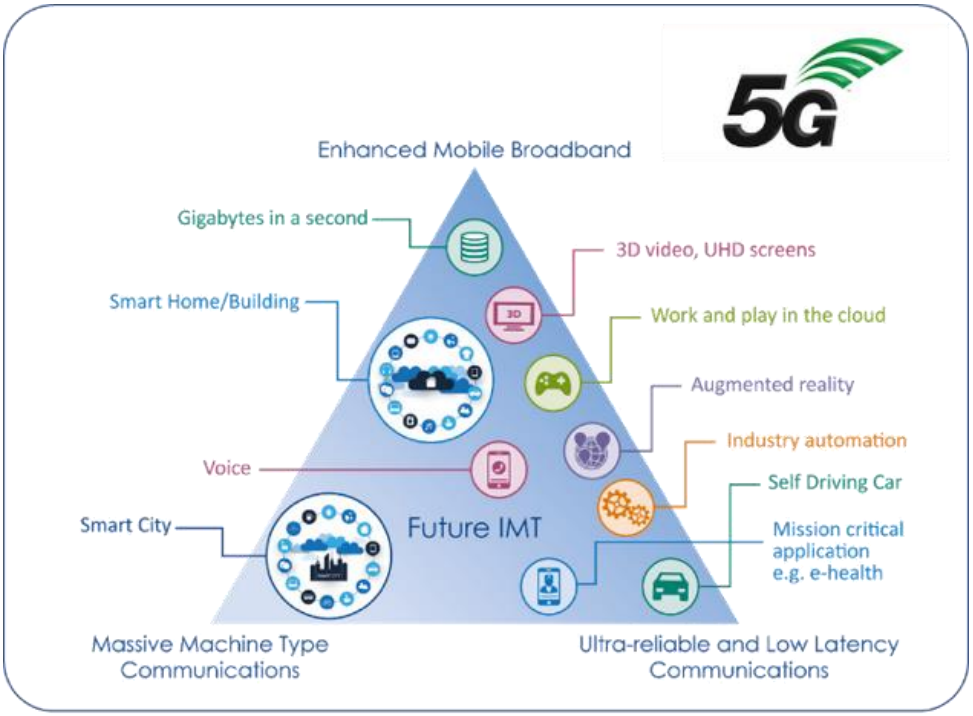
In onderstaande figuur zijn de generaties van netwerken weergegeven. In de afgelopen 40 jaar is er elke 10 jaar een nieuwe generatie van de mobiele communicatietechnologie in de publieke mobiele netwerken geïmplementeerd. Op basis van deze waarneming mag worden verwacht dat rond 2030 de volgende generatie, 6G, beschikbaar zal komen.



Figuur 6. Ontwikkeling van generaties binnen de mobiele technologie

De 3GPP werkt met een release planning waarin de standaarden worden vastgelegd; op dit moment wordt aan de standaarden van release 17 gewerkt (gereed in eind 2021). Met release 15 (uitgebracht in juni 2018) is de eerste versie van 5G specificatie beschikbaar gekomen. Als er een release van een standaard door 3GPP is uitgegeven, duurt het over het algemeen ongeveer twee jaar voordat deze standaard door leveranciers in het netwerk en ook in de mobiele devices is ingebouwd. De eerste, op release 15 gebaseerde 5G- oplossingen, zijn nu op de markt beschikbaar. Of de missiekritische functies met dezelfde doorlooptijd beschikbaar komen is de vraag; voor de operators vormen deze functies een nichemarkt, waar wellicht minder prioriteit aan wordt gegeven.

De 5G-technologie zal de komende periode breder beschikbaar komen in de mobiele netwerken van de Nederlandse MNO's. In de navolgende figuur is weergegeven wat de belangrijkste kenmerken zijn van de 5G-technologie ten opzichte van de 4G-technologie.



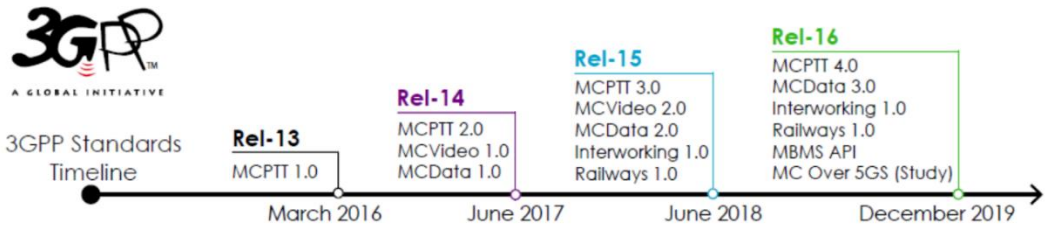
Figuur 7. 5G-toepassingsgebieden

Er worden drie ontwikkelgebieden onderkend:

1. Enhanced Mobile Broadband: dit is een vervolg op 4G waarbij er in 5G meer bandbreedte beschikbaar komt ten opzichte van 4G;
2. Massive Machine Type Communications: dit zijn toepassingen zoals IoT (internet of Things) waarbij grote volumes aan sensoren kleine hoeveelheden data versturen;
3. Ultra Reliable Low Latency Communications: de missiekritische mobiele breedbandcommunicatie is hier een voorbeeld van.

De netwerken van de drie mobiele operators in Nederland zijn op dit moment gebaseerd op een combinatie van 2G (GSM), 3G (UMTS) en 4G (LTE). De 2G- en 3G-netwerken zullen binnen afzienbare tijd verdwijnen; de Nederlandse operators zijn hier al mee gestart. De uitrol van 5G-netwerken loopt op dit moment in Nederland. Vodafone is de eerste MNO in Nederland die 5G-technologie in het operationele mobiele netwerk landelijk heeft geactiveerd op bestaande 4G-frequenties.

Binnen de 3GPP-standaarden zijn sinds release 13 (uitgebracht in 2016), naast de generieke functies, ook zogenoemde missiekritische functies gestandaardiseerd. In iedere release sinds release 13 zijn er nieuwe missiekritische functies aan de standaarden toegevoegd. Binnen 3GPP is de werkgroep SA-6[3] verantwoordelijk voor de ontwikkeling van deze MCX-standaarden. Vanuit Nederland neemt een vertegenwoordiger van de Nederlandse politie deel aan de werkgroep voor de ontwikkeling van deze standaarden. In de navolgende figuur zijn MCX-functies op hoofdlijnen per release weergegeven.



Figuur 8. MCX-functies gerelateerd aan de 3GPP release, bron 3GPP zie www.3gpp.org

De standaardisatie-ontwikkeling van de MCX-functionaliteiten over een 5G netwerk moeten nog starten en zullen pas vanaf release 17 beschikbaar komen. Release 17 wordt volgens de huidige planning in december 2021 uitgebracht. De verwachting is dat missiekritische MCX-functies niet vóór 2024 op een operationeel 5G-netwerk mogelijk zijn. Voor 4G zijn de eerste releases van MCX-functies gebaseerd op de releases 13, 14 en 15 inmiddels beschikbaar. De verwachting is dat de MCX-functies van release 16 begin 2022 beschikbaar komen.

De huidige op de markt beschikbare 3GPP-gestandaardiseerde MCX-functies zijn dus op 4G-technologie gebaseerd. Nog niet alle functies die in de TETRA-standaard zijn opgenomen, zijn op een vergelijkbaar missiekritisch niveau beschikbaar in 3GPP-technologie. Een voorbeeld is de zogenaamde DMO (Direct Mode Operation) functie in TETRA. Dit is een functie in de TETRA-portofoon waarbij er, indien de radiodekking van het TETRA-netwerk volledig is weggevallen, een fall back mogelijkheid aanwezig is om direct tussen portofoons onderling te communiceren zonder tussenkomst van het netwerk. In 3GPP (4G) is geprobeerd deze functie te creëren, genoemd ProSe (proximity-based services), maar dit biedt niet een vergelijkbare oplossing. Afhankelijk van de uiteindelijke eisen van de OOV-organisaties kan dit een risico vormen voor de acceptatie van de missiekritische mobiele breedband oplossing.

De MNO's in de wereld bepalen zelf in hoeverre ze de missiekritische functies ook als dienst (zullen) aanbieden aan hun klanten. Dat geldt ook voor de MNO's in Nederland. Om missiekritische functies in mobiele netwerken toe te voegen, zijn veelal additionele investeringen in de netwerken noodzakelijk. Ze stellen ook andere eisen aan de beheerorganisatie dan die voor de MNO's bekende massamarkt. Dit betreffen met name eisen op het gebied van veiligheid en een gegarandeerde, hogere beschikbaarheid.

[3] 3GPP MCX update; brondocument nr. 64

3.6 Ontwikkeling in beveiliging

3.6.1 Inleiding

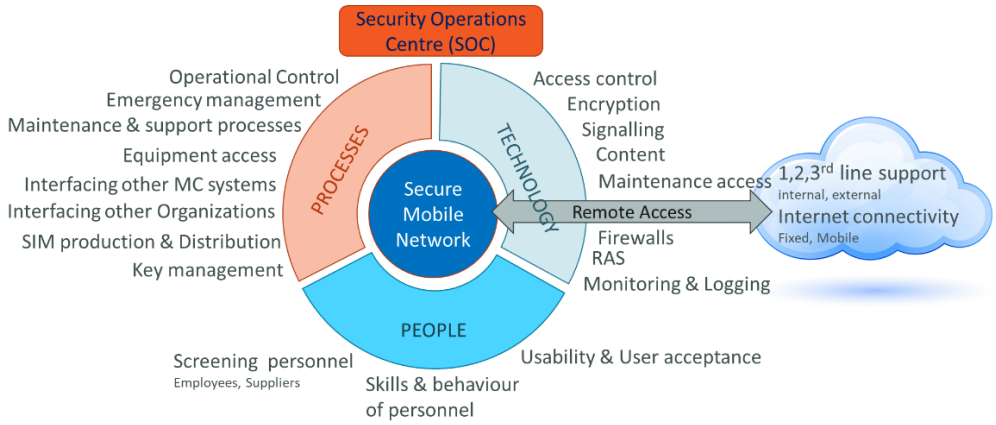
De beveiligingscomponent van missiekritische netwerken hebben we gesplitst in de netwerkbeveiliging en de informatiebeveiliging. Hierbij is de netwerkbeveiliging gericht op de beveiliging van de toegang, alleen geauthentiseerde gebruikers krijgen toegang tot het mobiele netwerk, de beveiliging van de radio interface, het transmissienetwerk en het core-netwerk. De informatiebeveiliging heeft betrekking op de informatie van gebruikerstoepassingen en signaleringsinformatie van gebruikers die over het mobiele netwerk getransporteerd wordt.

Daarnaast is er nog de beveiliging die zorg draagt voor de continuïteit en de beschikbaarheid van de dienstverlening. Deze beveiliging is gericht tegen fysieke bedreigingen zoals opzettelijke radiosignaalverstoring (jamming), vernielingen van apparatuur. Hoewel dit zaken zijn waar serieus rekening mee moet worden gehouden, zijn dit externe verstoringen waar in de standaard geen maatregelen voor worden ontworpen. Dit vergt andersoortige passende maatregelen.

3.6.2 Netwerkbeveiliging

3.6.2.1 Algemeen

De beveiliging van een missiekritisch breedband netwerk of het gebruik van een missiekritische dienst op een breedbandnetwerk strekt zich verder uit dan alleen de technologie en de systemen. Voor een integrale benadering van de netwerkbeveiliging spelen naast de technologie ook het inrichten van de beveiligingsprocessen en de menselijk factoren een belangrijke rol om tot een adequaat beveiligingsniveau van de totale oplossing te komen. In onderstaande figuur wordt de integrale aanpak van beveiliging van een mobiel netwerk schematisch weergegeven.



Figuur 9. Integrale benadering van de beveiliging van mobiele breedbandnetwerken

Binnen de 4G-technologie van 3GPP-netwerken is de beveiligingsmethode gestandaardiseerd. De beveiliging richt zich met name op toegangscontrole, authenticatie, autorisatie en de encryptie van de mobiele verbinding. De SIM-kaart (fysiek of e-sim) speelt in deze beveiliging nog steeds een essentiële rol. Op de SIM-kaart is beveiligingsinformatie opgeslagen die samen met de beveiligingsinformatie in het core-netwerk zorg dragen voor de technische beveiliging.

De beveiliging van het transmissienetwerk is door de 3GPP gestandaardiseerd op basis van IPsec (Internet Protocol Security) voor 4G. Voor een goede beveiliging moet de netwerkeigenaar (MNO) deze beveiliging dan wel toepassen

om inbreuk op het netwerk te voorkomen. Het core-netwerk wordt in een beschermde omgeving geplaatst waarbij alleen geautoriseerde personen toegang krijgen tot de systemen voor het onderhoud en beheer. De koppelvlakken naar externe netwerken worden beveiligd met firewalls om ongeautoriseerde toegang tot het netwerk te voorkomen.

Binnen het mobiele breedband netwerk wordt ook netwerkinformatie (signalering) gebruikt waarbij het zichtbaar is waar gebruikers zich in het mobiele netwerk bevinden en met wie ze in contract zijn. Deze informatie behoort in een missiekritisch netwerk ook tot vertrouwelijke informatie waarvoor adequate beveiligingsmaatregelen genomen moeten worden. Dit kan onder andere door de informatie af te schermen van het normale netwerkverkeer en alleen voor geautoriseerde personen toegankelijk te maken.

Bij de verdere uitwerking van de missiekritische breedband oplossing zijn de beveiligingsaspecten zowel bij de verwerving, de implementatie als ook gedurende de operationele fase van belang.

3.6.2.2 Internationale roaming

Doordat 3GPP-technologie zijn oorsprong vindt in de mobiele operatormarkt, waarbij internationale roaming een belangrijke functionaliteit is, beschikken alle mobiele openbare en niet-openbare op 3GPP gebaseerde netwerken over een zogenoemde MCC (mobile country code, 3 digits) en MNC (mobile network code, 3 digits) code. Voor Nederland is de MCC-code 204. Ieder 3GPP-netwerk dat gekoppeld is met een ander netwerk heeft een MNC-code. Op basis van deze code zijn de 3GPP-netwerken wereldwijd te identificeren.

Bij het gebruik van een eigen netwerk voor een missiekritische toepassing zijn de daarop uitgegeven SIM-kaarten voorzien van een IMSI (International Mobile Subscriber Identity), welke bestaat uit de MCC, MNC en een tiencijferig subscriber nummer. Bedacht moet worden dat als een gebruiker met een dergelijke SIM-kaart in het buitenland verbinding zoekt met een ander netwerk (roaming), deze gebruiker op basis van de MNC herkend kan worden als zijnde een gebruiker van een missiekritisch netwerk. Voor sommige gebruikstoepassingen kan dit een operationeel veiligheidsrisico voor de gebruiker betekenen.

Bij 5G zijn additionele beveiligingsmogelijkheden toegevoegd ten opzichte van 4G, waarbij de identiteit wordt verstopt door gebruik te maken van een tijdelijke en versleutelde identiteit. In 5G wordt deze mogelijkheid SUCI (SUbscription Concealed Identifier) genoemd waarmee de identiteit van de gebruiker zowel op het eigen 5G netwerk maar ook op een roaming netwerk beveiligd kan worden.

3.6.2.3 Inhoudelijke technische beveiliging

De beveiliging binnen de TETRA-standaard wordt over het algemeen (nog) als goed beschouwd. Deze beveiliging richt zich zowel op de netwerk beveiliging als ook op de beveiliging van het randapparaat en de spraakapplicatie. Binnen de TETRA-standaarden is de beveiliging, de communicatiefuncties, de spraak- en data-applicatie zowel voor het netwerk als het randapparaat gestandaardiseerd. Binnen TETRA vindt al enige tijd op dit gebied geen ontwikkeling meer plaats.

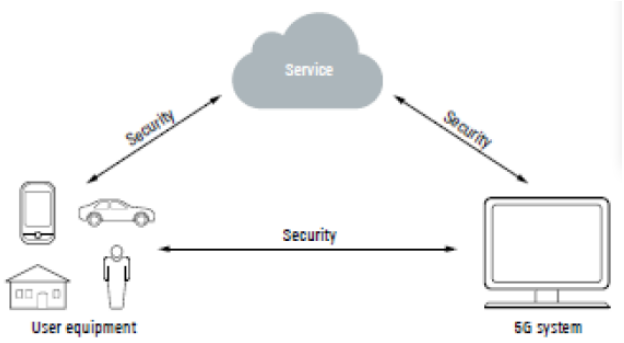
De opbouw van mobiele breedbandnetwerken is op dit punt afwijkend ten opzichte van een TETRA-netwerk; in mobiele breedbandnetwerken zijn het netwerk en de toepassing van elkaar gescheiden. De beveiliging van een mobiel breedbandnetwerk beperkt zich dan ook tot alleen het netwerk. Voor de toepassing en het randapparaat moeten additionele maatregelen genomen worden om de beveiliging van de gehele keten te waarborgen. De onderstaande tabel geeft een vergelijking weer tussen TETRA enerzijds en 3GPP 4G-technologie anderzijds voor de toegang tot het netwerk, de beveiliging van de radio interface, de beveiliging van de communicatie inhoud, de toepassing en de beveiliging van het mobiele randapparaat.

Bij een mobiel breedbandnetwerk kan de beveiliging op een vergelijkbaar goed niveau ingericht worden als bij een TETRA-netwerk; er zijn echter wel additionele maatregelen nodig in de vorm van additionele encryptie en beheer-systemen voor mobiele randapparaten zoals MDM- (mobile device management) en MAM- (mobile application management) tools.

	TETRA	3GPP
Netwerk Toegang	Wederzijdse authenticatie	Wederzijdse authenticatie
Radio interface beveiliging	Encryptie met dynamische sleutels van signalering en data verkeer	Encryptie met dynamische sleutels van signalering en data verkeer
Content (spraak en groep) communicatie beveiliging end to end	Specifieke maatregel in mobile device/ radio bediening	Specifieke maatregel in mobile device/ radio bediening
Applicaties	Geintegreerd in netwerk	Netwerk en applicatie laag
Security device	Geintegreerd	MDM en MAM tools noodzakelijk

Figuur 10. Vergelijking beveiliging TETRA vs 3GPP 4G

Naar de toekomst gezien zijn er binnen de 3GPP-standaard met 5G meer beveiligingsmogelijkheden beschikbaar. Bij 5G kunnen naast de beveiligingsfuncties uit 4G ook de service/applicatie beveiliging geïntegreerd worden in de oplossing. In onderstaande figuur is dit schematisch weergegeven.



Figuur 11. 5G biedt ook applicatiebeveiligingsmogelijkheden, bron Rohde&Schwarz

De integrale beveiliging van de gehele keten van het mobiele netwerk, mobiele devices en de applicaties is essentieel voor de uiteindelijke missiekritische toepassing die in het veld gebruikt gaat worden. In dit onderzoek is de reikwijdte beperkt tot alleen het netwerkonderdeel; mobiele devices en applicaties vallen buiten reikwijdte van dit onderzoek.

3.6.3 *Informatiebeveiliging*

De informatiebeveiliging van de informatie van gebruikerstoepassingen en signaleringsinformatie van gebruikers die over het mobiele netwerk getransporteerd wordt, start met het rubriceren van de informatiebeveiligingsniveaus. We hebben voor het onderzoek de uitgangspunten van de Nederlandse politie genomen[4].

Ten aanzien van informatiebeveiliging zijn er binnen de politie vier rubriceringsniveaus gedefinieerd: Politie intern, Politie confidentieel, Politie geheim, Politie zeer geheim.

Voor het digitaal verzenden van informatie zijn er algemene richtlijnen opgesteld ten aanzien van het vertrouwelijkheidsniveau van de informatie. In het algemeen wordt er verwezen naar de adviezen van de Werkgroep Bijzondere Informatiebeveiliging (WBI) van de politie. Voor de rubricering van Politie interne informatie geldt voor communicatievoorzieningen:

- Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.
- Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen (zero footprint). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt:
    - Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen;
    - Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten en indien mogelijk het toestel gewist.

Voor een toekomstig missiekritisch mobiele breedbandnetwerk moet nader onderzocht en gespecificeerd worden welke maatregelen noodzakelijk zijn voor de informatiebeveiliging van de hogere rubriceringsniveaus. Voor de goede orde, de andere OOV-organisaties kennen vergelijkbare classificaties als die van de politie, die wij als voorbeeld hebben gebruikt.

3.7 Ontwikkelingen in Nederland

In Nederland hebben de mobiele netwerk operators de afgelopen drie jaar voorbereidingen getroffen om de 5G-technologie in hun mobiele netwerken te implementeren. Vodafone heeft als eerste operator in april 2020 deze technologie landelijk operationeel gemaakt. De andere twee operators zullen naar verwachting binnenkort volgen.

3.7.1 *Veiligheid*

In de aanloop naar de introductie van 5G-technologie in Nederland is er een politieke discussie ontstaan over de bedreiging door statelijke actoren met een offensief beleid tegen de Nederlandse staat. In de Tweede Kamer is er gesproken over de invloed van deze statelijke actoren en de gevaren voor de Nederlandse samenleving. De vitale

[4] Informatiebeveiliging politie en veiligheidsregio's, brondocumenten nr. 54 en 55

infrastructuren zijn hierbij als potentieel risico aangewezen. De mobiele telecommunicatienetwerken in Nederland zijn onderdeel van deze vitale infrastructuren.

Op 28 november 2019 is er een Algemene Maatregel van Bestuur (https://zoek.officielebekendmakingen.nl/stb-2019-457.html) "Besluit veiligheid en integriteit telecommunicatie" door de ministers van EZK en van JenV afgekondigd waarbij de mobiele operators in Nederland verplicht kunnen worden om maatregelen te nemen tegen de veiligheidsdreigingen op de (toekomstige) mobiele telecommunicatienetwerken in Nederland. Voor de mobiele operators levert dit een lastig dilemma op bij de ontwikkeling van hun 5G-netwerken. Er zijn op basis van de AMvB nog geen leveranciers uitgesloten, zodat de operators bij investeringen in hardware en software telkens de afweging moeten maken of er een kans bestaat dat de betreffende leverancier later alsnog wordt uitgesloten.

De AMvB is niet alleen van toepassing op publieke mobiele netwerken en diensten maar ook op missiekritische diensten. Het is niet duidelijk of de AMvB wel afdoende is voor deze missiekritische diensten of dat er aanvullende maatregelen nodig zijn.

3.7.2 Frequenties en spectrumbehoefte

Het frequentiebeleid in Nederland is de verantwoordelijkheid van het ministerie van EZK. Het frequentiespectrum is een zeer schaarse "grondstof" voor mobiele netwerken. Binnen Nederland is er een frequentieplan waarin alle frequenties zijn opgenomen met de bijbehorende toepassing en gebruiker(s). Het ministerie van EZK verdeelt het frequentiespectrum dat gebruikt wordt voor publieke mobiele netwerken de laatste twee decennia via een veilingmethodiek; dit is wettelijk vastgelegd als primaire verdelingsmethodiek van schaarse frequenties. De MNO's in Nederland kunnen door deelname aan de veilingen het benodigde spectrum verwerven voor een bij de veilingvoorwaarden bepaalde periode. In juni 2020 zal er een nieuwe multiband veiling plaats vinden voor frequenties in 700, 1.400 en 2.100 MHz, waarbij naast reeds eerder uitgegeven frequenties, ook nieuwe, voor 5G-netwerken bedoelde frequenties worden geveild. In 2022 zal een veiling plaatsvinden voor de 3,5 GHz band, bedoeld voor 5G.

Voor het ministerie van JenV is er in het frequentieplan van Nederland binnen de 700MHz band – naast de 2x30 MHz voor de veiling in juni 2020 – ook 2x 5MHz en 2x 3MHz, dus in totaal 2x 8MHz, gereserveerd voor een toekomstig mobiel breedbandnetwerk voor OOV-organisaties. Dit spectrum is bedoeld als een aanvulling op de dienstverlening uit de markt. Dit spectrum is niet beoogd, en ook niet voldoende, voor een volwaardig eigen netwerk.

In de 400MHz-band heeft het ministerie van JenV momenteel spectrum in gebruik voor het huidige C2000-netwerk, dit is 2x 5MHz in de 380-400MHZ-band en 2x 1,5MHz in de 410-430MHz-band. Standaard randapparatuur voor de massamarkt is veelal niet geschikt voor deze frequenties. Hiervoor is specifieke randapparatuur nodig. Daarnaast is onzeker of dit spectrum de komende 15 jaar beschikbaar zal blijven voor de OOV-organisaties.

De bovengenoemde hoeveelheid frequentiespectrum die nu gereserveerd en in gebruik is voor de OOV-organisaties (2x 8MHz), is niet toereikend om die totale behoefte voor de OOV-organisaties in de komende 5 tot 15 jaar af te dekken. De inschatting van de spectrumbehoefte hebben we nader uitgewerkt.

3.7.2.1 Uitwerking frequentiespectrum behoefte

Zowel voor een eigen missiekritisch mobiel breedbandnetwerk (scenario 1) als ook bij het gebruik van het netwerk van een mobiele operator (scenario's 2 en 3) is er behoefte aan frequentiespectrum. TNO heeft in 2017 onderzoek

gedaan naar onder andere de bandbreedtebehoefte voor OOV-organisaties[5]. Hierbij heeft TNO een aantal gebruiksscenario's uitgewerkt die wij als uitgangspunt hebben genomen om de behoefte aan frequentiespectrum te kunnen inschatten. Bij missiekritische toepassingen is er een aanzienlijk verschil tussen de behoefte in een normale operationele situatie en die in het geval van calamiteiten. De eigenschap van calamiteiten is dat vooraf niet te voorspellen is waar een calamiteit zich zal voordoen en wat de consequentie is voor de belasting van het netwerk. Bij het ontwerpen van een mobiel netwerk moet er dus van uitgegaan worden dat een calamiteit zich overal kan voordoen en dat dan de benodigde capaciteit voorhanden is. De meest kritische locatie voor een mobiel netwerk is aan de rand van een netwerkcel; daar is de beschikbare capaciteit slechts ongeveer 10% van de capaciteit direct naast het antenne-opstelpunt. Daarnaast zal ook voor de normale, niet-calamiteit situatie een gegarandeerde minimale capaciteit aan de rand van een netwerkcel beschikbaar moeten zijn.

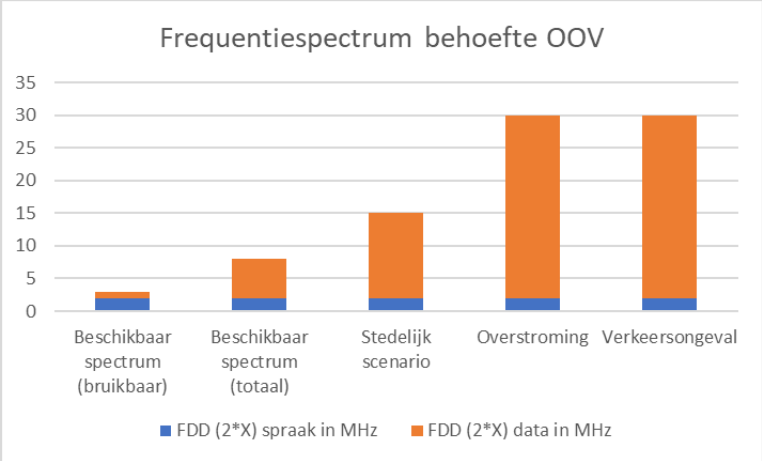
Voor de behoefte aan spectrum zijn er drie scenario's door TNO uitgewerkt: 1. Stedelijke omgeving; 2. Een overstromingsramp; 3. Een verkeersongeval.

De behoefte aan bandbreedte per scenario is:

- Stedelijk scenario: UL (Uplink) 2.6Mbps, DL (Downlink) 2.1Mbps per cel
- Overstroming scenario: UL 6.6Mbps, DL 3.1Mbs per cel
- Verkeersongeval scenario: UL 6,6Mbps, DL 3,1Mbs per cel
- Spraak: UL 0,5Mbps, DL 0,5Mbps per cel

In bijlage A4 is de frequentiespectrum behoefte in detail uitgewerkt.

In onderstaande grafiek is het beschikbare spectrum en de spectrumbehoefte voor de verschillende TNO scenario's grafisch weergegeven in MHz voor spraak- en data toepassing indien gebruik gemaakt wordt van FDD (Frequency Division Duplex) technologie.



Figuur 12. Beschikbaar spectrum en OOV-behoefte aan spectrum

[5] Rapport TNO Facilitering missie-kritisch mobiel breedband voor het OOV-domein; brondocument 36

De uitwerking betreft een globale inschatting van de spectrum behoefte die nog nader uitgewerkt dient te worden op basis van uitgangspunten en criteria die van invloed zijn op de kwaliteit van het netwerk. Hierbij is het ook mogelijk om de spectrum behoefte te optimaliseren en daarbij bijvoorbeeld concessies te doen aan de uitgangspunten.

De behoefte aan spectrum zal in de toekomst met de groei van breedbandtoepassingen steeds verder toenemen. In scenario 1 waarbij de Nederlandse overheid een eigen mobiel breedbandnetwerk gaat aanleggen, is voldoende eigen spectrum de eerste harde randvoorwaarde. Dit spectrum moet liggen in een of meer frequentiebanden waarin een 4G/5G-ecosysteem beschikbaar is of binnenkort beschikbaar komt en in heel Nederland beschikbaar zijn.

De conclusies van het benodigde frequentiespectrum voor missiekritische mobiel breedbandtoepassing zijn:

- Het benodigde frequentiespectrum om het piek verkeer te kunnen faciliteren minimaal 2x30MHz (bij FDD-technologie) of 45MHz (bij TDD-technologie).
- Van beschikbare spectrum in de 700MHz band (2x8MHz) is op dit moment 2x3MHz bruikbaar en voor de 2x5MHz is op dit moment nog geen eco systeem van apparatuur op de markt beschikbaar. Indien dit eco systeem de komende 3 jaar zich ontwikkelt zou een basisvoorziening met het beschikbare spectrum gerealiseerd kunnen worden waarmee spraak functionaliteit met 0,5Mbps en zeer beperkte data functionaliteit met een bandbreedte van 1,5Mbps gefaciliteerd kan worden.
- Op dit moment is er onvoldoende frequentiespectrum gereserveerd om een landelijk dekkend mobiel breedbandnetwerk voor missiekritische OOV-toepassing te kunnen realiseren. Als deze randvoorwaarde niet ingevuld kan worden, dan is scenario 1 niet haalbaar.

3.7.3 Netneutraliteit en prioriteit

In de Nederlandse telecommunicatie wetgeving zijn de EU-regels uit de verordening 2015/2120 opgenomen inzake netneutraliteit. Deze regels verbieden aanbieders van openbare telecommunicatienetwerken om onderscheid te maken in hun dienstverlening richting gebruikers en richting dienstenleveranciers. Voor de missiekritische communicatiebehoefte binnen de overheid is een uitzondering gemaakt: voor “gespecialiseerde diensten” is het mogelijk om prioriteit te geven aan deze vorm van communicatie over een publiek netwerk. De Autoriteit Consument en Markt (ACM) staat ervoor open dat OOV-organisaties onder bepaalde omstandigheden toegang, prioriteit en capaciteit krijgen boven andere partijen, zoals bij een crisis en binnen een beperkt gebied en tijd. Precieze criteria ontbreken vooralsnog, wat het voor MNO’s lastig maakt om in te schatten hoe zij hieraan kunnen voldoen zonder door de ACM op de vingers te worden getikt. Zie ook paragraaf 3.7.5.

3.7.4 Behoefte ontwikkeling van OOV-organisaties

De behoefte aan mobiele breedbandtoepassingen voor de OOV-gebruikers is onderzocht door TNO[6]. De verwachting is dat de OOV-gebruikers breedbandtoepassingen verder operationeel willen inzetten ook in missiekritische omgeving. In de huidige situatie maken de OOV-organisaties voor de invulling van de mobiele breedband behoefte gebruik van de standaard diensten van de mobiele operators (MNO’s), naar verwachting ook al in missie kritische situaties. Om in de toekomst in de groeiende behoefte aan missie kritische mobiele breedbandtoepassingen te kunnen voldoen is het zaak om tijdig in te spelen op de realisatie van een missiekritische breedband netwerk-oplossing.

[6] TNO monitor draadloze technologie, najaar 2019; brondocument nr. 4

3.7.5 *Opstelling en verwachting van de MNO's in Nederland*

Het ministerie van JenV heeft in november 2017 een marktconsultatie uitgevoerd onder de mobiele netwerk operators in Nederland. In deze consultatie heeft het ministerie een hybride mobiele breedband oplossing getoetst met een gedeeltelijk eigen netwerkoplossing en gedeeltelijk ingekochte dienst bij mobiele operators. De mobiele operators hebben aangegeven positief te staan tegenover een hybride model. De voorkeur van de partijen gaat uit naar een commerciële aanpak, bestaande uit het contracteren van bepaalde quality of service afspraken, in plaats van het voorschrijven ervan via wet- en regelgeving (zoals bijvoorbeeld de overloop van netwerkcapaciteit naar MNO-netwerken in val van calamiteiten). Het grote voordeel van contracten is dat deze zich meer lenen voor flexibiliteit dan wet- en regelgeving. De mobiele operators zijn van mening dat het mogelijk is om commercieel in de toekomstige capaciteitsbehoefte van de OOV-organisaties te voorzien. De mate waarin het kan worden ingevuld verschilt per operator. De mobiele operators zien een oplossing met de inzet van de publieke mobiele netwerken voor missiekritische toepassing als haalbaar. Er zijn wel aandachtspunten in het rapport[7] vermeld:

- De netneutraliteit, zoals beschreven in 3.7.3, is een punt van aandacht. De operators zien de regelgeving op dat vlak momenteel nog als onvoldoende duidelijk en daarmee als een beperking. Zij willen geen onnodig risico lopen met de ACM, maar kunnen ook niet elk gesprek of elke verkeersstroom controleren. Een voorbeeld is dat niet al het verkeer via elk missiekritisch device daadwerkelijk missiekritisch is en in alle gevallen prioriteit hoort te krijgen.
- Realisme ten aanzien van het stellen van eisen in verband met verouderde randapparatuur.
- Overvraag de markt niet. Door een eventuele opdracht te veel te specificeren ontstaat het risico dat oplossingen die de operators reeds in ontwikkeling hebben, niet passen. Daarnaast wordt het risico gesignaleerd dat het opleggen dan wel aangaan van te veel verplichtingen een te zware last creëert voor de bestaande klanten van de operators.
- Door aan te sluiten bij internationale ontwikkelingen wordt voorkomen dat een specifiek Nederlandse oplossing ontstaat. Als een land een eigen oplossing heeft, die afwijkt van die van de buurlanden, dan belemmert dat de onderlinge samenwerking en uitwisselbaarheid.
- Er is tijd nodig voor het uitvoeren van de transitie. Met name het overzetten van de apparatuur bij eindgebruikers kost veel tijd. Daarom is tijdig starten van belang. Tevens moet er rekening mee worden gehouden dat door de voorziene transitietijd mogelijk langere tijd twee systemen naast elkaar moeten worden gebruikt.

3.8 EU-ontwikkelingen

Binnen de EU loopt op dit moment het zogenaamde BroadWay initiatief, van de PSCE (Public Safety Communications Europe) organisatie (www.psc-europe.eu), waaraan 11 EU-landen, waaronder Nederland, deelnemen. BroadWay is een pre-commercial procurement (PCP) ontwikkelprogramma dat gefinancierd wordt door de EU. Het initiatief is gestart met BroadMap, waarin de functionele behoefte van public safety organisaties in Europe is geïnventariseerd. Dit is de basis geweest voor de gelijknamige tender die in 2019 in de markt is gezet.

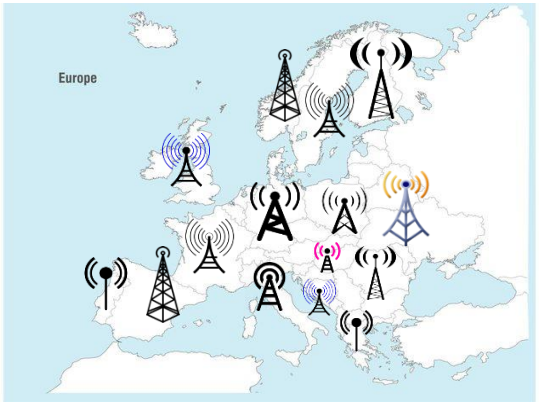
[7] Ministerie van JenV algemene bevindingen marktconsultatie breedband OOV, sept 2018; brondocument nr. 59

Het doel van het BroadWay-programma[8] is om public safety organisaties uit verschillende landen in Europa beter met elkaar te laten samenwerken. Op basis van BroadWay kunnen deze organisaties internationaal met elkaar communiceren via een pan-Europees netwerk. Dit pan-Europese netwerk komt tot stand doordat in de toekomst elk deelnemend Europees land een mission critical mobiel breedbandnetwerk gebruikt, dat gebaseerd is op de 3GPP-standaarden. BroadWay verzorgt de connectiviteit tussen de mobiele breedbandnetwerken om grensoverschrijdend te kunnen werken. Het programma kent 3 fasen en heeft in september 2019 geleid tot de selectie van 4 consortia die in concurrentie fase 1 hebben afgerond met een ontwerp voor het pan-Europese Public Safety netwerk.

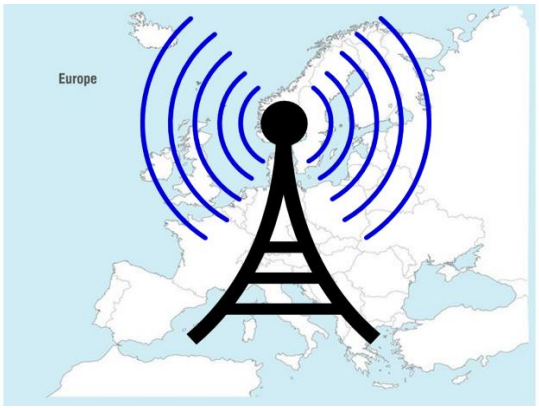
In fase 2 zal er een prototype gebouwd worden en in fase 3 zal er een pilot uitgevoerd worden met eindgebruikers. Fase 3 zal naar verwachting medio 2022 afgerond worden.

Nadat BroadWay afgerond is, waarbij de haalbaarheid van één (virtueel) pan-Europees missiekritisch breedbandnetwerk is aangetoond, zal er een selectie traject starten voor BroadNet. Hierin zal de pan-Europese public safety oplossing op basis van 3GPP voor operationeel gebruik gekozen, geïmplementeerd en in gebruik genomen worden. Dat zal naar verwachting na 2024 van start gaan. In de onderstaande twee figuren worden de huidige situatie, waarbij ieder Europees land een eigen netwerk heeft dat niet onderling gekoppeld is, en de toekomstige situatie in de visie van BroadWay, weergegeven. In die laatste is er met BroadNet functioneel gezien binnen Europa één pan-Europees breedbandnetwerk voor missiekritische toepassingen.

Huidig



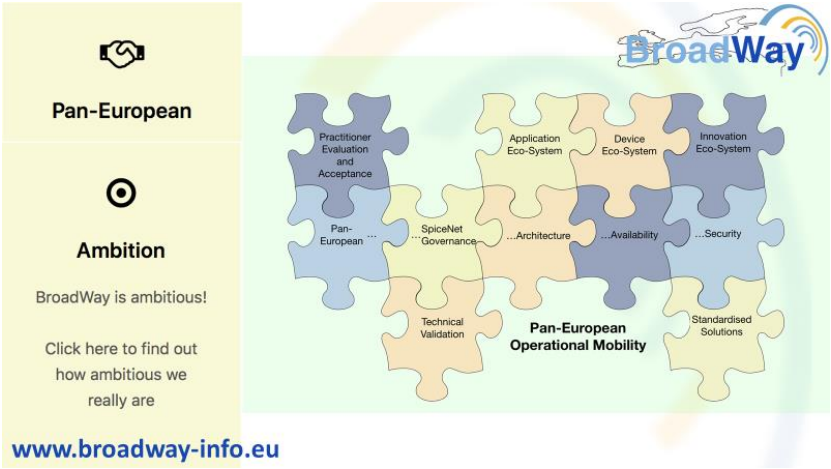
Toekomstig



Figuur 13. Huidig en toekomstig Europess missiekritisch netwerk, bron: Broadway

BroadWay betreft niet alleen de technologie om pan-Europees werken voor public safety organisaties mogelijk te maken; het betreft ook de processen en procedures om Europese landen met elkaar grensoverschrijdend samen te laten werken en ook de oplossing te kunnen (laten) beheren, waarbij de soevereiniteit van iedere lidstaat gehandhaafd blijft. BroadWay zal Europese aansluitvoorwaarden gaan opstellen waaraan de deelnemende landen zullen moeten voldoen om tot een pan-Europese netwerkoplossing te komen in BroadNet. Indien Nederland wil aansluiten met het Nederlandse missiekritische breedbandnetwerk op BroadNet zal het moeten voldoen aan de aansluitvoorwaarden van BroadNet.

[8] BroadWay informatie; brondocument nr. 39.



Figuur 14. De ambitie van BroadWay, bron Broadway

3.9 Landen met mobiele breedband implementatie

Een aantal landen is al bezig met de ontwikkeling en implementatie van missiekritische breedbandcommunicatie. Omdat voor ieder land de startpositie anders is qua politiek en organisatie (landelijk, staten, regionaal, lokaal) maar ook qua geografie, de leeftijd en mogelijkheden van de huidige systemen, de behoefte aan breedband voor informatieverwerking et cetera, is er ook variatie in de gekozen oplossingen en aanpak om de oplossingen te realiseren. Dat betekent ook dat er niet een standaard beste aanpak en oplossing zijn en ook geen blauwdruk die we in Nederland één-op-één kunnen overnemen. In de volgende paragrafen laten we een aantal initiatieven de revue passeren.

3.9.1 Verenigd Koninkrijk – Emergency Services Network

In het Verenigd Koninkrijk is in 2014 het ESN[9] (Emergency Services Network) gestart vanuit het programma ESMCP van het ministerie van Binnenlandse Zaken (Home Office). Het ESN is een mobiel breedbandnetwerk voor missiekritische communicatie gebaseerd op 3GPP 4G standaarden, met een separaat ESN core netwerk en gebruikmakend van het publieke radionetwerk van MNO EE. Het ESN maakt gebruik van het radionetwerk en het beschikbare frequentiespectrum van EE. De oorspronkelijke doelstelling van de Britse overheid was om in 2017 het oude, op TETRA-technologie gebaseerde netwerk te vervangen door ESN. Dit is echter niet gelukt. Er zijn veel aanloopproblemen geweest met ESN waardoor de gebruikers geen vertrouwen hadden in de ESN-dienstverlening. Op dit moment is het streven om het oude TETRA-netwerk in 2024 uit te schakelen.

Een belangrijke reden achter de gemaakte keuze voor de Britse overheid was destijds om de extreem hoge kosten van de bestaande dienstverlening (leverancier Airwave) te verlagen door de introductie van ESN. Doordat de vervanging van het TETRA-netwerk binnen de geplande termijn niet gelukt is en er gedurende meer dan zeven jaar een dubbel netwerk operationeel gehouden moet worden, is de kostendoelstelling bij lange na niet gehaald. In de jaarlijkse audit van de Britse overheid door IPA (Infrastructure and Project Authority) heeft ESN in 2018 de beoordeling “niet

[9] ESN informatie en status implementatie; brondocumenten nr.34, 51, 60, 62, 63, 65

haalbaar" gekregen en in 2019 "twijfelachtig of het doel gerealiseerd kan worden". Het oorspronkelijke budget is in 2019 al met 3,1 miljard pond overschreden en het project ligt drie jaar achter op het oorspronkelijke schema.

In het Verenigd Koninkrijk heeft de selectie van één MNO voor het missiekritisch netwerk tot de discussie geleid dat er mogelijk een verstoring van de concurrentie in de telecommunicatiemarkt heeft plaats gevonden. De geselecteerde MNO heeft met overheidssteun het publiek netwerk geoptimaliseerd qua radiodekking, kwaliteit en beschikbaarheid waardoor het ook in de consumentenmarkt een voordeel heeft gekregen ten opzichte van de concurrentie. Hoewel er geen duidelijkheid is of er feitelijk een verstoring heeft plaats gevonden, dient een overheid dit risico zeker mee te nemen in de overwegingen over deze oplossingsrichting.

3.9.2 US – FirstNet

In de Verenigde Staten is de ramp op 11 september (9/11) 2001 de trigger geweest om de missiekritische communicatie te onderzoeken in de 9/11 commissie. Dit heeft ertoe geleid dat in 2012 de First Responder Network Authority "FirstNet"[10] is opgericht. In 2017 heeft FirstNet via een PPP (Public Private Partnership) initiatief een 6,5 miljard dollar-contract met een looptijd van 25 jaar gegund via een aanbestedingsproces aan één MNO: AT&T. AT&T heeft vanaf dat moment public safety netwerkdiensten ontwikkeld op basis van de FirstNet specificatie op het 4G publieke mobiele breedband netwerk met een separaat core-netwerk. Onderdeel van het AT&T-contract is dat de Amerikaanse overheid frequentiespectrum (2x 10MHz FDD in LTE-band 14, de 700MHz-band) heeft toegewezen aan AT&T, waarbij AT&T dit spectrum onder normale omstandigheden mag gebruiken voor het publieke breedbandnetwerk en indien FirstNet dit spectrum nodig heeft dit dynamisch en met prioriteit wordt toegewezen aan de FirstNet-gebruikers.

De doelstelling van FirstNet is om een landelijk dekkende missiekritische mobiele breedbanddienst te creëren voor public safety gebruikers. Dit netwerk is opgebouwd naast de bestaande P25-netwerken. De status op dit moment is dat FirstNet 2,74 miljoen vierkante "miles" radiodekking in de VS heeft wat ongeveer 99% dekking van de bevolking inhoudt, 76% geografische dekking en in totaal 1,2 miljoen gebruikers/mobiele devices heeft. Public safety organisaties in de VS kunnen zelf kiezen of zij willen aansluiten op FirstNet. Er is een tarief model (rateplan) geïntroduceerd op SIM-niveau waardoor er een lage drempel is tot toetreding. Het rateplan start bij ongeveer 40 dollar per maand per SIM.

AT&T is verantwoordelijk voor de dienstverlening en ook het life cycle management van de dienst om bijvoorbeeld van 4G over te stappen naar 5G-technologie. Naast het netwerk heeft FirstNet ook een app store geïntroduceerd voor missiekritische applicaties. Voor deze app store is een certificeringsproces van toepassing. Er is met deze keuze een ecosysteem van toepassingen ontstaan.

3.9.3 Zuid-Korea

In Zuid-Korea is ook een missiekritisch mobiel breedbandnetwerk geïntroduceerd voor de missiekritische organisaties gebaseerd op 3GPP 4G-technologie. In 2015 en 2016 is een pilot gedaan in drie steden. MNO SK Telecom levert deze dienstverlening en het Koreaanse Samsung is de leverancier van het netwerk en de missiekritische applicaties. Voor het netwerk wordt gebruik gemaakt van zogenoemde RAN-sharing, het gemeenschappelijk gebruik van het radionetwerk, met de MNO waarbij 2x 10MHz in de 700MHz-band specifiek voor public safety is toegewezen door

[10] FirstNet informatie; brondocumenten nr. 32, 41, 47, 66

de Koreaanse overheid. In 2018 is tijdens de Olympische winterspelen een 2e pilot gedaan. De landelijke uitrol is in 2019 gestart en wordt naar verwachting in 2020 afgerond.

3.10 Andere landen die verder in de voorbereiding zijn dan Nederland

3.10.1 Finland Virve 2.0

In Finland is Erillisverkot, een overheidsorganisatie, de leverancier van Virve, de missiekritische dienstverlening voor de public safety gebruikers. Virve 1.0 is een landelijk dekkend TETRA-netwerk dat in eigendom van de overheid is. Met Virve 2.0[11] heeft Finland de richting voor mobiel breedband bepaald gebaseerd op de 3GPP 4G/5G technologie. De strategische keuzes die door de Finse overheid gemaakt zijn in Virve 2.0, zijn vervolgens in 2019 met een aanbestedingsproces uitgevraagd. Kortgeleden is het resultaat van deze aanbesteding bekend gemaakt. Finland heeft ervoor gekozen geen specifiek spectrum ter beschikking te stellen ten behoeve van het missiekritische breedbandnetwerk. Dit betekent dat het mobiele breedbandnetwerk wordt gebouwd op basis van 3GPP 4G/LTE-technologie met de dienstverlening van het radionetwerk van één bestaande MNO inclusief gebruik van het spectrum van deze MNO. Voor het core-netwerk wordt een eigen netwerk gebouwd, waarvoor de leverancier inmiddels is geselecteerd. Dit core-netwerk zal geleverd gaan worden door een Europese leverancier. De looptijd van het contract voor Virve 2.0 is 10 jaar. In Finland is er in het aanbestedingsproces een maximumprijs per SIM als uitgangspunt gehanteerd als randvoorwaarde die ingegeven is door de gebruikersorganisaties om deel te nemen aan Virve 2.0. Deze maximumprijs ligt tussen de €25 en €40 per SIM per maand.

Nederland kan de ervaringen die opgedaan zijn in Finland projecteren op de Nederlandse situatie. Er zijn wel verschillen tussen Finland en Nederland. Finland is qua oppervlakte achtmaal groter dan Nederland en heeft ten opzichte van Nederland driemaal minder inwoners. In Finland is het gebruik van mobiele breedband diensten in de massamarkt aanzienlijk hoger dan het gebruik in Nederland. Met gemiddeld 20GB per SIM per maand behoort Finland tot de grootste gebruikers in de wereld. Het gebruik in Nederland is gemiddeld 2,7GB per SIM per maand[12].

3.10.2 Duitsland BDBOS

In Duitsland is BDBOS[13] de overheidsorganisatie die de huidige missiekritische communicatiediensten levert op basis van TETRA-technologie. In Duitsland is het grootste TETRA-netwerk ter wereld operationeel met meer dan 4600 antenneopstelpunten en meer dan 800.000 mobiele randapparaten.

BDBOS heeft voor de opvolger gekozen voor een hybride oplossing op basis van mobiel breedband gebaseerd op de 3GPP standaard. Deze oplossing bestaat uit een gedeeltelijk eigen netwerk dat gebruik maakt van eigen spectrum in de 450 MHz-band (2x 10MHz bandbreedte) en de 700 MHZ-band (2x 8MHz bandbreedte) en maakt daarnaast gebruik van het radionetwerk van de mobiele operators in Duitsland. Duitsland kiest er bij mobiel breedband voor om de basiscapaciteitsbehoefte af te gaan dekken in een eigen overheidsnetwerk (waarbij de keuze voor 450MHz, in de wereld uniek is) en voor de piekcapaciteitsbehoefte gebruik te gaan maken van de diensten van operatornetwerken.

---

[11] Virve informatie; brondocumenten nr. 38, 53, 56, 57

[12] Tefficient gemiddeld datagebruik per maand; brondocument nr. 61

[13] BDBOS informatie; brondocument nr. 42

Afgelopen jaar is de voorbereiding van een “broadband test” van de hybride oplossing gestart, die in 2020 zal worden uitgevoerd.

3.10.3 Frankrijk PCSTORM

Na de terroristische aanslagen in 2015 heeft het ministerie van Binnenlandse Zaken in Frankrijk een traject gestart voor de toekomst van missiekritische mobiele breedband communicatie gebaseerd op de 3GPP standaard. In 2017 heeft er een selectieproces plaats gevonden voor het zogenaamde PCSTORM-project. PCSTORM[14] is een ontwikkel-project waarin een consortium van verschillende bedrijven en één mobiele netwerk operator de toekomstige oplossing heeft gedefinieerd, gebaseerd op een oplossing met eigen frequentiespectrum in de 700MHz-band (2x 8MHz). De uitvoering van het project door het consortium is begin 2019 van start gegaan. De oplossing bestaat uit een integratie van netwerk, applicaties en mobiele devices.

Het is de bedoeling dat public safety organisaties in Frankrijk de oplossing gaan testen. Deze testen staan voor 2020 gepland.

3.10.4 Noorwegen

In 2017 heeft de overheid in Noorwegen besloten dat er geen frequentiespectrum wordt gereserveerd voor een overheidseigen missiekritisch breedbandnetwerk en daarmee in de toekomst gebruik te gaan maken van de netwerken en diensten van de mobiele operators in Noorwegen.

In Noorwegen is in de periode 2005-2015 een eigen TETRA-netwerk opgebouwd onder de naam Nødnett met 2100 base stations en 55.000 mobiele randapparaten. Dit netwerk is eigendom van de Noorse overheid en het operationeel beheer is uitbesteed tot eind 2026. In Noorwegen is in 2018 onderzoek[15] gedaan naar de optimale oplossing voor een toekomstig breedbandnetwerk ten aanzien van de verantwoordelijkheden verdeling tussen de Noorse overheid en de commerciële mobiele netwerk operators. Het onderzoek is in nauw overleg met de drie mobiele operators in Noorwegen uitgevoerd.

De volgende eisen zijn aan het toekomstige netwerk gesteld:

- Radiodekking overal (ook in tunnels, air-ground communicatie, op afgelegen locaties met weinig commerciële potentie);
- Hoge betrouwbaarheid en beschikbaarheid, ook ingeval van grote incidenten, extreme weersomstandigheden, rampen;
- Hoog data beveiligingsniveau en bescherming tegen cyberattacks
- Gespecialiseerde functionaliteit, zoals groepscommunicatie, communicatie op locaties zonder radiodekking.

Er zijn 3 scenario’s geïdentificeerd:

1. Secure MVNO; de overheid heeft zijn eigen core-netwerk waarop alle radionetwerken van de mobiele operators worden aangesloten.
2. Volledig uitbestede dienst bij één mobiele operator

[14] PCSTORM informatie; brondocument nr. 43

[15] Nødnett, DSB rapport Next Generation Network; brondocument nr. 37

3. Volledig uitbestede dienst bij meerdere concurrerende mobiele operators

De voor- en nadelen van de scenario's zijn onderzocht. De belangrijkste bevindingen zijn:

- Een core-netwerk dat in eigendom is van de overheid, inclusief onderhoud en beheer door de overheid, geeft de meeste controle.
- Een uitbestede dienst kan ook de optie in zich hebben om een separate core in te richten los van het operator core-netwerk. Dit heeft als voordeel dat slechts een kleine groep beheerpersonen toegang heeft tot sensitieve netwerkinformatie.
- Een oplossing met de radionetwerken van alle operators geeft een iets betere radiodekking dan indien het netwerk van één operator wordt gebruikt.
- Het toepassen van de radionetwerken van meerdere operators is complexer dan het toepassen van het radionetwerk van één operator.
- Indien de overheid gaat investeren in de kwaliteitsverbetering van mobiele netwerken van operators zouden alle operators moeten mee profiteren van deze investering om marktverstoring te voorkomen (als voorbeelden worden genoemd: redundante transmissie, extra dekking door extra base stations, extra stroomvoorziening om onderbrekingen op te vangen).
- De dialoog met de operators helpt om tot de goede keuzes te komen.

In Noorwegen is de overheid in het besluitvormingsproces van de scenariokeuze en loopt iets voor op de situatie in Nederland.

3.10.5 België

In België is er een missiekritische TETRA-netwerk van de overheid operationeel. Astrid is de overheidsorganisatie die de missiekritische communicatie aan de OOV-organisaties in de vorm van dienstverlening aanbiedt. De OOV-organisaties in België maken al enige tijd gebruik van mobiele breedbandcommunicatie (4G) onder de naam "Blue Light Mobile". Dit is een mobiele dienst die Astrid[16] afneemt van de Belgische operators. Op het moment dat het netwerk van één mobiele operator uitvalt, wordt automatisch een verbinding gemaakt met het netwerk van een andere mobiel operator (Base of Orange). Op het netwerk van de mobiele operator Proximus biedt deze dienst prioriteit boven het normale, publieke, mobiele verkeer. Bovendien biedt Astrid in deze dienst een extra end-to-end beveiliging over de mobiele verbinding. Deze dienst is echter geen missiekritische dienst; het biedt geen garanties van beschikbaarheid, kwaliteit, performance en radiodekking. Een SIM-dienst met 8GB bundel inclusief spraak kost €6,- per SIM per maand. De Belgische overheid is in een vergelijkbare afwegingsfase over de toekomst van missiekritische breedband als Nederland.

[16] Zie voor meer informatie www.astrid.be

4 ONDERZOEK TOEKOMSTSCENARIO'S

4.1 Inleiding

Zoals beschreven in het hoofdstuk Opzet haalbaarheidsonderzoek, bestaat de aanpak van het onderzoek uit de volgende stappen:

- Bepalen van de toekomstscenario's;
- Opstellen van de criteria (inclusief de subcriteria) en de scoremethodiek;
- Bepalen van de weging van de (sub)criteria;
- Uitvoeren van de evaluatie;
- Bepalen van de rangorde van de toekomstscenario's;

4.2 Overwegingen bij het onderzoek

Na het bepalen van de toekomstscenario's, de beoordelingscriteria en de wegingsfactoren is de analyse van de scenario's tegen de beoordelingscriteria uitgevoerd. Daarbij is een aantal overwegingen naar voren gekomen die we in de navolgende paragrafen nader toelichten.

4.2.1 Tijd

Het uitgangspunt bij de beoordeling van de scenario's is de situatie over ongeveer vijf tot tien jaar later, dus de periode van 2025 tot 2035. Verder dan 2035 kijken is in het kader van dit onderzoek weinig zinvol omdat er te veel variabelen zijn die te onzeker zijn om nog voor dit onderzoek waardevolle uitspraken te kunnen doen.

We hebben op basis van de beschikbare documentatie in kaart gebracht wat de redelijke verwachtingen zijn ten aanzien van de drie scenario's in de genoemde periode en daarbij zoveel mogelijk gelijke voorwaarden gehanteerd zodat de scenario's maximaal vergelijkbaar zijn.

De informatie van het 0-scenario betreft de huidige situatie. Deze is niet geprojecteerd op de periode 2025-2035 omdat het 0-scenario geen doelscenario is en uitsluitend wordt gebruikt ter vergelijking.

4.2.2 Financiën

In de eerste opzet was 'Financiën' één van de criteria binnen de multicriteria-analyse inclusief een weegfactor. Tijdens het onderzoek hebben we in overleg met de opdrachtgever besloten om financiën uit het weegmodel te halen en per scenario apart weer te geven. De ratio hiervoor is drieledig:

1. De afweging tussen geld en kwaliteit (waar onder ook veiligheid) is vooral een bestuurlijke afweging die afhankelijk van onder andere politieke en actuele ontwikkelingen tot andere overwegingen en uitkomsten kan leiden. Het vastleggen van een 'vaste' weegfactor doet geen recht aan deze situatie.
2. De afgelopen maanden (van crisisbeheersing als gevolg van COVID-19) hebben duidelijk gemaakt dat de waarde van geld en financiering door externe omstandigheden razendsnel ingrijpend kan wijzigen. Ook dat is een reden om terughoudend te zijn met het vastleggen van een weegverhouding tussen geld en andere factoren.
3. Uit het onderzoek kwam naar voren dat kosten en investeringen van de drie scenario's zeer sterk uiteenlopen. Daarmee wordt het criterium financiën dermate dominant, dat het te veel het onderscheidend vermogen van de andere factoren verhult.

4.2.3 Risico's en kansen

Bij de beoordeling van de scenario's hebben we verschillende risico's gesignaleerd. Deze zijn in eerste instantie per subcriterium opgenomen en meegewogen in de beoordeling. Daarnaast zijn de belangrijkste risico's verzameld in een apart criterium Risico's en Kansen waarin een overzicht van de risico's is gecreëerd per scenario. Met name de risico's die op meerdere criteria van invloed zijn, hebben we in dit criterium beoordeeld.

Hetzelfde hebben we gedaan voor de mogelijke kansen die bij een scenario horen. Bij de beoordeling bleken die echter veel minder aanwezig te zijn.

4.2.4 Frequenties

Bij de beoordeling van het criterium Frequenties hebben we de volgende aspecten in overweging genomen:

- Is het spectrum in voldoende mate beschikbaar, voldoende voor voorzienbaar toekomstig gebruik?
- Wordt het spectrum efficiënt gebruikt of wordt (een deel van) het spectrum alleen ingezet bij situaties die zeer zelden en waarschijnlijk ook gedurende beperkte tijd voorkomen zoals grootschalige incidenten?
- Wat zijn de voor- en nadelen van een scenario en de daarvoor benodigde frequenties met betrekking tot kosten en doorlooptijden voor de realisatie van het radionetwerk?
- Is er sprake van spectrum in de frequentiebanden die ook voor de massamarkt wordt ingezet, zodat standaard devices en onderdelen kunnen worden gebruikt? Of worden er afwijkende frequenties gebruikt?
- Welke consequenties hebben de te gebruiken frequenties op de internationale samenwerking en uitwisseling met de ons omringende landen en andere landen in de wereld?

4.2.5 Binnenhuisdekking

Bij het subcriterium binnenhuisdekking speelt een aantal factoren een rol: De veldsterkte (hoe krachtig is het signaal?), de gebruikte frequentie (hoe hoger de frequentie, hoe minder die binnenshuis doordringt) en de speciale locaties. Deze laatste (Special Coverage Locations of SCL's genoemd) zijn door de overheid aangewezen locaties waarvan de eigenaar verplicht wordt om zorg te dragen voor voldoende indoordekking. Als de oplossing gebruik maakt van standaard frequenties (die ook door de commerciële operators worden ingezet), dan zijn de kosten voor de locatie-eigenaar beperkter dan wanneer andere frequenties worden gebruikt. Hoewel dit geen directe kosten voor de oplossing zijn, hebben we ze wel meegenomen in de overweging van dit subcriterium.

4.2.6 Beveiliging

Bij het criterium Beveiliging hebben we gekeken naar verschillende aspecten die van invloed zijn op de uiteindelijke veiligheid van de te realiseren oplossing. Daarnaast hebben we overleg gehad met vertegenwoordigers van de AIVD over de wijze waarop die organisatie de beveiliging beoordeelt. Dat dit onderwerp belangrijk is, blijkt uit de recente discussies in de Tweede Kamer over de huidige C2000-oplossing van Hytera en de mogelijke invloed die de Chinese regering daarop zou kunnen hebben. De AIVD heeft in hun analyse daarvan geconcludeerd dat het risico beperkt is en er geen reden is om de implementatie en gebruik te blokkeren.

Bij de beoordeling van de drie scenario's hebben we gekeken naar de volgende aspecten:

- Welke controle en invloed kan de overheid uitoefenen? Heeft de overheid alles in eigen hand of niet?
- Welke beveiligingsmiddelen zitten er in de oplossing zelf? En welke risico's?
- Wat doen operators aan beveiliging?
- Als de overheid afhankelijk is van andere partijen zoals MNO's, dan is er een vertrouwensband nodig. Hoe realistisch is dat?

De AIVD heeft aangegeven dat de beveiliging vooral moet uitgaan van de data en de informatie die mogelijk over het netwerk wordt verstuurd. Het vertrouwelijkheidsniveau van die data bepaalt uiteindelijk welke mate van beveiliging noodzakelijk is en of de door de oplossing geleverde beveiliging toereikend is. In het uiterste geval is de oplossing niet geschikt voor een dergelijke (zeer vertrouwelijke) gegevensstroom en zal een ander middel moeten worden ingezet. Zie voor vertrouwelijkheidsniveaus in de OOV ook paragraaf 3.6.3.

We willen erop wijzen dat de gegevens die over een netwerk worden verstuurd, niet alleen de te transporteren data betreft, zoals gesprekken, beelden, bestanden en dergelijke bevat, maar ook metagegevens. Dat zijn bijvoorbeeld locatiegegevens (de aanmelding van een device op een opstelpunt kan de positie van de betreffende gebruiker verraden) en verkeersgegevens die op zich informatie kunnen bevatten over het gebruik van de betreffende device/gebruiker. Deze informatie kan bij het gebruik van openbare 4G-netwerken lastiger worden afgeschermd, zeker in het geval van internationaal roamen, 5G biedt hier additionele mogelijkheden.

4.2.7 Kennis en kennisbehoud

Een belangrijke randvoorwaarde voor de realisatie van elk van de scenario's is dat de overheid beschikt over voldoende kennis, dus gekwalificeerd personeel met de juiste kennis van zaken. De exacte behoefte varieert per scenario: in scenario 1, waarin de overheid zelfstandig de netwerken inricht en beheert, zal vooral veel technische kennis nodig zijn. In scenario 2, waarin de overheid alles uitbesteedt, zal de nadruk liggen op meer high-level en regiekennis om de leveranciers te kunnen aansturen. In scenario 3 zal een mix van beide nodig zijn.

De overheid zal in elk van de drie scenario's moeten zorgen voor de verkrijgen van die kennis en voor het behouden ervan. Dat laatste is een minstens zo grote uitdaging omdat diepe technische kennis schaars is en zeer gevraagd door marktpartijen die zich in deze mobiele breedband branche bewegen.

4.2.8 Tijdslijnen

Als we kijken naar de tijdslijnen voor de realisatie van de drie scenario's, dan zijn er grofweg een negental delen te onderscheiden:

1. **Bestuurlijke besluitvorming en BIT-toets**: Er zal een keuze voor een bepaalde oplossing moeten worden gemaakt inclusief financiering die bestuurlijk wordt goedgekeurd, waarbij een BIT-toets noodzakelijk zal zijn. Dit geldt voor elk van de drie scenario's. Voor scenario 1 ligt deze stap op het kritieke pad, terwijl bij de andere twee de ontwikkeling van de 4G- en 5G-netwerken door de operators onderwijl doorloopt en geen vertraging ondervindt.

2. **Aanbestedingen**: In elk van de scenario's zal de overheid meerdere aanbestedingen moeten uitvoeren om de eindoplossing te realiseren. Gezien de complexiteit van de totaaloplossing kan het tijdsbeslag hiervoor oplopen tot twee à drie jaar.

3. **Realisatie van de antenne-opstelpunten**: Dit is in elk van de scenario's een tijdrovende stap. Er moeten relatief veel antenne-opstelpunten bijkomen om de benodigde dichtheid te realiseren. De vergunnings-procedure per antenne-opstelpunt verschilt soms per gemeente en kost relatief veel tijd. De marktervaring in Nederland op dit moment is dat het gemiddeld 2 jaar duurt voordat een nieuwe antenne-opstellocatie verworven is. De aanvraagprocedure en de procedures om tegen de aanvraag in beroep te gaan nemen veel tijd in beslag. Wij schatten in dat er in scenario 1 ongeveer 700 volledig nieuwe antennelocaties nodig zullen zijn naast de 1600 bestaande locaties. Vervolgens zal naar deze nieuwe locaties ook een transmissieverbinding en elektriciteit moeten worden aangelegd waarvoor de nodige graafwerkzaamheden moeten plaats-vinden. Vooral in stedelijke gebieden is dit lastig en tijdrovend. Een voordeel zou kunnen zijn dat de overheid

de huidige C2000-opstelpunten kan inbrengen voor de operators om ook daar opstelpunten te kunnen realiseren. Voor scenario 2 en 3 wordt gebruik gemaakt van de bestaande radionetwerken van de operators. Bij deze twee scenario's is alleen nog aanvullende radiodekking noodzakelijk op de locaties waar operators op dit moment nog geen dekking hebben gerealiseerd. Dit betreft echter maar een beperkt aantal nieuwe antennelocaties.

4. **Inrichten van het transmissienetwerk**: Bij scenario 1 moet naast het complete radionetwerk ook het transmissie netwerk aangelegd worden. Omdat dit als dienst wordt ingekocht zal dit door toeleveranciers worden gerealiseerd. Uitrol hiervan loopt in belangrijke mate synchroon met de uitrol van de opstelpunten, maar met name eventueel graafwerk kan voor veel vertraging zorgen. Een belangrijk besluit betreft de in te richten redundantie per opstelpunt. Bij scenario 2 en 3 wordt van de bestaande transmissie netwerken van de operators gebruik gemaakt. Bij de meeste operators is elk opstelpunt met één fysieke verbinding aangesloten op het transmissienetwerk. In het huidige C2000-netwerk is maar ongeveer 10% van de opstelpunten met twee gescheiden fysieke routes (en dus redundant) aangesloten. Als die redundantie, via gescheiden routes, een eis wordt voor meer (of zelfs alle) opstelpunten, dan zullen er extra verbindingen moeten worden aangelegd, waarbij veelal graafwerk komt kijken, wat (veel) extra doorlooptijd kan vergen.

5. **Inrichten van het core-netwerk**: In de scenario's 1 en 3 richt de overheid het eigen core-netwerk in. In scenario 2 voert één van de operators die taak uit voor de overheid. In scenario 2 is er nog een keuze of er van de standaard aanwezig core-netwerk gebruik gemaakt wordt of dat er een voor deze toepassing separaat core-netwerk door de operator wordt aangelegd. Indien dat vereist is zal dat bij de operator sneller gaan, vanwege de reeds aanwezige ervaring met bestaande core-netwerken bij de operators.

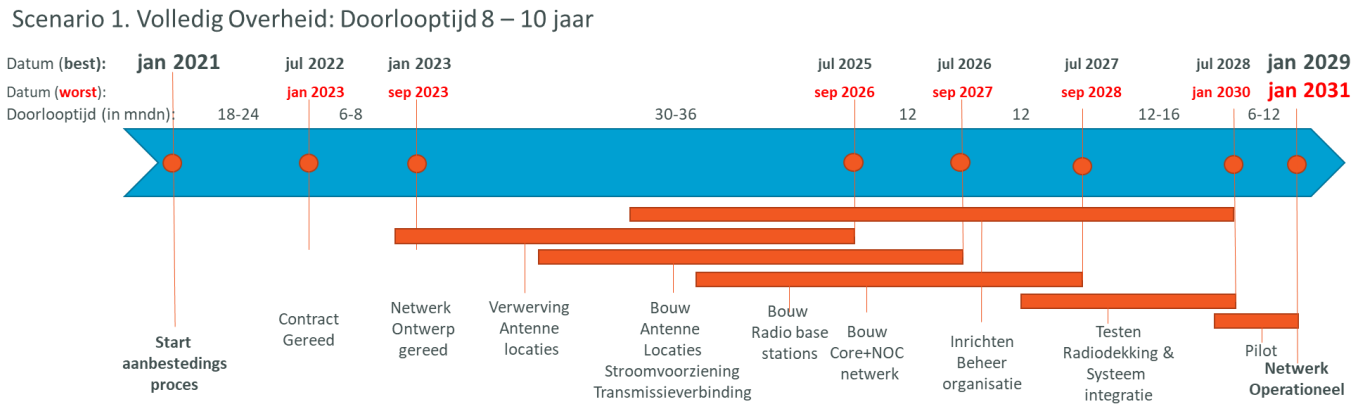
6. **Verkrijgen van de frequenties**: Met name in scenario 1 speelt het verkrijgen van voldoende frequentiespectrum een essentiële rol. Grofweg zijn er twee methoden voor de overheid om over spectrum te kunnen beschikken. Allereerst kan de overheid via de BOP-procedure zichzelf het benodigde spectrum toewijzen. Deze kent een driejaarlijkse cyclus. Bij de laatste keer (2017) is de in paragraaf 3.7.2 aangegeven 2x 8MHz toegewezen. Ten tweede kan de overheid spectrum inkopen (huren) bij de bestaande operators. Ook combinaties van beide zijn denkbaar. Bij de scenario's 2 en 3 zal de overheid RAN-capaciteit als dienst inkopen inclusief het benodigde spectrum. De doorlooptijden van de twee opties verschillen. De BOP-procedure kan zo'n twee tot drie jaar duren. Het gebruik van spectrum via de diensten van de operators is de snelste vorm, omdat het in de scenario's 2 en 3 geen extra tijd vergt, anders dan het opstellen van de goede vraagspecificatie. Ten slotte kan er gedacht worden aan de mogelijkheid dat de overheid zelf bij de veiling meebiedt op de frequenties. Dit is echter geen reële optie omdat de overheid niet rechtmatig met publiek geld en als organisator van de veiling met commerciële partijen kan concurreren in een veiling.

7. **Inrichten van de beheerorganisatie**: in alle 3 de scenario's zal er een beheerorganisatie voor de missiekritische oplossing noodzakelijk zijn. In scenario 1 en 3 heeft de overheid zelf de beheerverantwoordelijkheid over het eigen netwerk (1) of alleen het core-netwerk (3). De overheid heeft op dit moment niet voldoende kennis in huis op het gebied van mobiele breedbandnetwerken en zal dus medewerkers moeten opleiden en op de arbeidsmarkt werven. Voor het beheer van een missiekritisch netwerk is specifieke beheerkennis noodzakelijk en tevens dienen er specifiek beheerprocessen te worden ingericht. Voor het inrichten van de beheerprocessen vormt het ITIL-service management model een goede basis daarnaast zijn er specifieke radiobeheerprocessen die ingericht moeten worden. De verwachting is dat het opbouwen van een beheerorganisatie jaren in beslag zal nemen. Voor scenario 2 en 3 worden ook diensten van operators ingekocht. Voor deze diensten zal een regie organisatie moeten worden ingericht om tot een goede beheerafstemming te komen van de eigen organisatie met de dienstenleverancier.

8. **Testen en pilot**: Tijdens het bouwen van het netwerk in scenario 1 en 3 zullen deeltesten plaats vinden. Nadat de implementatie volledig gereed is zullen er integratie en radionetwerktesten plaats vinden. Voor scenario 1 geldt dit voor het totale overheidsnetwerk, voor scenario 3 geldt dit voor het core-netwerk en de integratie met het radionetwerk van 1 MNO. In scenario 2 en 3 zullen er ook testen van de diensten van de operators plaats vinden. In scenario 2 met 3 MNO's zullen er ook integratietesten met de netwerken van alle 3 de operators gaan plaats vinden. Nadat de testen afgerond is er een pilot met gebruikers voorzien. Na de pilot wordt het netwerk c.q. de dienst operationeel.

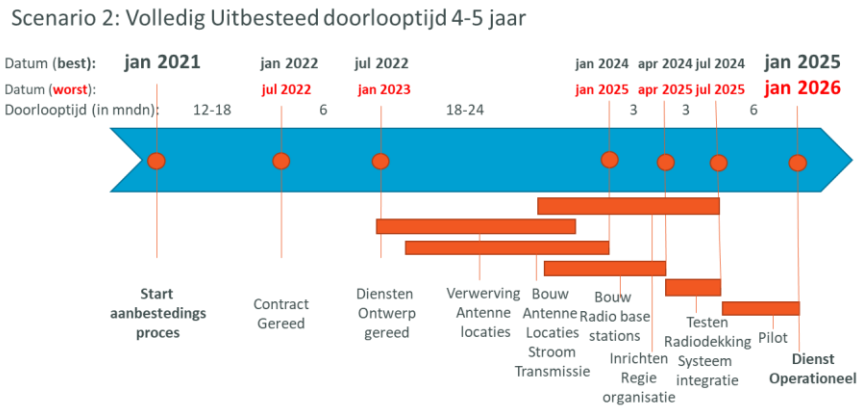
9. **Migratie**: De laatste stap in de realisatie is de migratie naar de nieuwe oplossing. Afhankelijk van de gekozen migratiestrategie kunnen het huidige C2000-netwerk en de missiekritische mobiele breedband oplossing kort of gedurende langere periode naast elkaar operationeel zijn. Dit hangt ook af van het functioneel samenwerken van C2000 met de nieuwe oplossing. De gebruikersacceptatie van de missiekritische oplossing is een cruciale voorwaarde in het bepalen van de migratiestrategie, hier kan veel geleerd worden van ervaringen in het buitenland. Bij scenario 1 kan pas gemigreerd worden als het hele netwerk gereed is. Bij scenario 2 en 3 zijn hier meer gefaseerde migratiemogelijkheden omdat hier gebruik gemaakt worden van bestaande netwerken van operators. Een eerste schatting van een voorzichtige migratie, met een geleidelijke overgang, geeft een doorlooptijd van 6 maanden tot 2 jaar.

In onderstaande figuren zijn de tijdslijnen per scenario weergegeven. Het betreft hier een globale inschatting. We zijn bij de tijdslijnen van een oplossing uitgegaan zonder redundant transmissie netwerk. De tijdslijnen zijn weergegeven tot het moment van operationele oplevering van het netwerk en of dienst. Na dit moment zal de migratie starten.



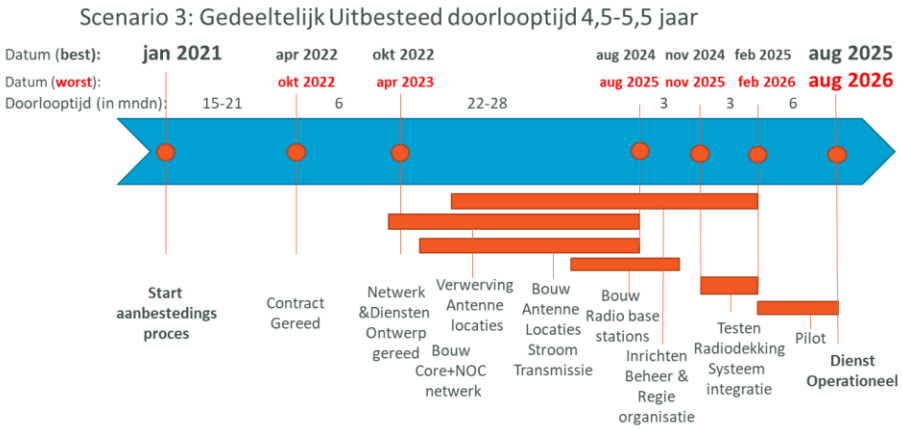
Figuur 15. Inschatting doorlooptijd scenario 1

Voor scenario 1 zijn het verwerven van de benodigde antenne-opstellocaties en het realiseren van het radio- en transmissienetwerk de activiteiten die een lange doorlooptijd vergen. We zijn hierbij uitgegaan dat het netwerk meer dan 2300 opstelplaatsen nodig heeft en dat er ongeveer 700 volledig nieuwe opstellocaties gecreëerd moeten worden. De aangegeven doorlooptijd kan verkort worden door te zoeken naar mogelijkheden om meer bestaande antennelocaties te gebruiken en door de vergunningsaanvraagprocedure te versnellen. Een langere doorlooptijd, meerdere jaren, is aangehouden voor het inrichten van de beheerorganisatie. Voor het testen en piloten is bij scenario 1 meer tijd nodig dan bij de scenario's 2 en 3.



Figuur 16. Inschatting doorlooptijd scenario 2

In scenario 2 is de verwerving van additionele antenne-opstellocaties voorzien om de radiodekking te verhogen; we zijn uitgegaan van in totaal 150 nieuwe locaties verdeeld over de 3 MNO's. De doorlooptijd kan verkort worden door de vergunningsaanvraagprocedure te versnellen. Het is in dit scenario goed mogelijk om te starten met de bestaande radiodekking[17] van de drie MNO's en de additionele dekking op een later moment op basis van behoefte in te richten. Hiermee kan een aanzienlijke verkorting van de doorlooptijd gerealiseerd worden (1-1,5 jaar). Het inrichten van een missiekritische dienst bij MNO's heeft een aanzienlijk kortere doorlooptijd dan het realiseren van een overheidseigen netwerkoplossing zoals in scenario 1.



Figuur 17. Inschatting doorlooptijd scenario 3

In scenario 3 heeft het inrichten van de beheerorganisatie van het core-netwerk een lange doorlooptijd. Verder is de verwerving van additionele antenne-opstellocaties voorzien om de radiodekking te verhogen; we zijn uitgegaan van

[17] In de eisen die horen bij de veiling van frequenties voor nieuwe mobiele communicatie uit 2020 wordt als eis gesteld 98% radiodekking per gemeente (geografisch). Zie ook: https://zoek.officielebekendmakingen.nl/stcrt-2020-13725.html

in totaal 100 nieuwe locaties bij één MNO. De doorlooptijd kan verkort worden door de vergunningsaanvraagprocedure te versnellen. Het is in dit scenario goed mogelijk om te starten met de bestaande radiodekking van de één MNO (met 95% radiodekking) en de additionele dekking op een later moment op basis van behoefte uit te breiden. Hiermee kan een verkorting van de doorlooptijd gerealiseerd worden (0,5-1 jaar). Het inrichten van een missiekritische dienst bij een MNO en een eigen core-netwerk heeft een aanzienlijk kortere doorlooptijd dan het realiseren van een volledig overheid-eigen netwerkoplossing zoals in scenario 1.

5 RESULTATEN ONDERZOEK

5.1 Inleiding

De multicriteria analyse is in het onderzoek voor de 3 toekomstscenario's uitgevoerd. De detailresultaten zijn in een separaat document elektronisch beschikbaar. Zie hiervoor bijlage A5. In dit hoofdstuk geven we de resultaten van het onderzoek in de vorm van:

- Het totaaloverzicht van de kwalitatieve beoordeling
- De resultaat business case, met hierin opgenomen de financiële vergelijking tussen de scenario's
- De voor- en nadelen per scenario
- Een overzicht van de belangrijkste risico's
- Mogelijkheden om de business case te beïnvloeden

5.2 Overzicht (Dashboard)

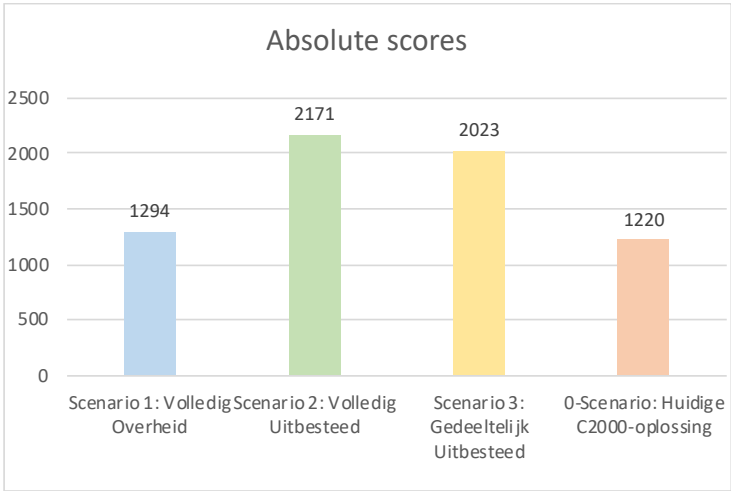
Zoals in het vorige hoofdstuk beschreven, is elk van de drie doelscenario's op 13 criteria (en 52 subcriteria) beoordeeld en vergeleken met het 0-scenario. De score (het aantal punten) voor elk scenario op elk individueel criterium ligt tussen de 0 en 100. Deze punten worden telkens vermenigvuldigd met de weegfactor van het betreffende criterium om de gewogen score uit te rekenen.

In het onderstaande overzicht zijn de resultaten van de kwalitatieve analyse per scenario en criterium weergegeven, waarbij per scenario voor elk criterium het aantal punten als ook de gewogen score is vermeld. Verder staan er onderaan de sommaties van de punten en de gewogen scores. Ten slotte staan er de relatieve gewogen scores ten opzichte van het absolute maximum en het scenario met de hoogste score.

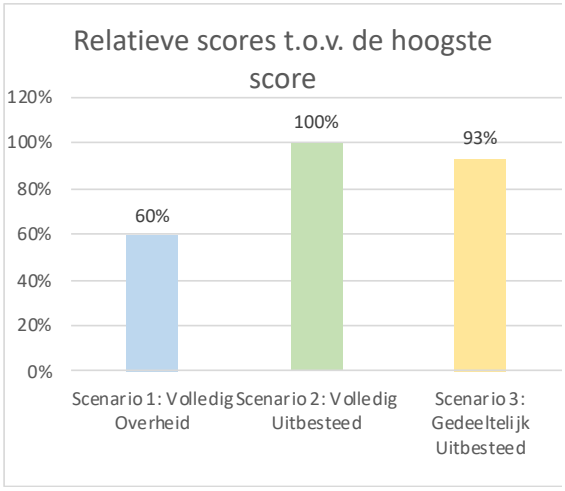
Behoefte	Weging	Scenario 1: Volledig Overheid		Scenario 2: Volledig Uitbesteed		Scenario 3: Gedeeltelijk Uitbesteed		0-Scenario: Huidige C2000-oplossing	
	1-3	Punten	Gewogen	Punten	Gewogen	Punten	Gewogen	Punten	Gewogen
1. Strategisch / politiek	1	77,5	77,5	52,5	52,5	72,5	72,5	57,5	57,5
2. Techniek	3	78,8	236,3	80	240	76,3	228,8	62,5	187,5
3. Beveiliging	3	85	255	60	180	67,5	202,5	65	195
4. Innovatie en toekomstvastheid	1	90	90	90	90	90	90	0	0
5. Frequentie spectrum	3	0	0	100	300	100	300	93,8	281,3
6. Organisatie	3	25	75	75	225	50	150	37,5	112,5
8. Besturing	2	70	140	70	140	70	140	40	80
9. Juridisch	1	92,5	92,5	100	100	85	85	95	95
10. Tijd / planning	2	20	40	75	150	75	150	25	50
11. Internationaal	3	50	150	90	270	95	285	5	15
12. Migratie	2	50	100	90	180	75	150	45	90
13. Risico's	3	12,5	37,5	81,3	243,8	56,3	168,8	18,8	56,3
Totaal	**27**	**651,3**	**1293,8**	**963,8**	**2171,3**	**912,5**	**2022,5**	**545**	**1220**
Relatieve score tov beste:		**60%**		**100%**		**93%**		**Dit is geen breedband-oplossing**	
Relatieve score tov max:		**48%**		**80%**		**75%**			
Rang:		**3**		**1**		**2**			

Figuur 18. Totaaloverzicht resultaten multicriteria-analyse

Zoals uit dit overzicht blijkt, liggen de scenario's 2 en 3 qua haalbaarheid redelijk dicht bij elkaar. Scenario 2 heeft een licht hogere overall score. Scenario 1 blijft ver achter op de andere twee. Zie ook de navolgende twee grafieken waarin de scores per scenario absoluut en relatief zijn weergegeven.



Figuur 19. Absolute score van de scenario's



Figuur 20. Relatieve score van de scenario's

Voor de duidelijkheid: in deze scores zijn de financiële cijfers (kosten en investeringen) niet meegenomen.

5.3 Resultaat beoordeling kwalitatieve criteria

Hoewel scenario 2 *Volledig Uitbesteed* overall de hoogste score heeft, betekent dit niet dat scenario 2 automatisch in de onderzochte vorm het voorkeurscenario is. Het is goed om na te gaan op welke onderdelen scenario 2 goed scoort en op welke onderdelen het scenario nog kan worden aangevuld en/of verbeterd.

De criteria die de doorslag geven bij de score van scenario 2 zijn:

- ***Frequentiespectrum***: Zowel in scenario 2 en 3 is voldoende spectrum beschikbaar, zowel in dagelijkse operatie als in een crisissituatie met een piekbehoefte. Het spectrum wordt ook efficiënt gebruikt. Het gebruikmaken van de radionetwerken van alledrie de mobiele operators leidt tot de meest optimale benutting van het beschikbare frequentiespectrum, waardoor scenario 2 net beter scoort dan scenario 3.
- ***Organisatie*** (verwerving en beheer): In scenario 2 kan volledig gebruik worden gemaakt van de kennis en ervaring van de mobiele operators. Bij scenario 1 en 3 zijn onderdelen of de gehele infrastructuur in eigendom van de overheid. De overheid heeft niet de kennis en ervaring om een eigen complexe mobiele breedband oplossing te verwerven en beheren.
- ***Tijd/Planning***: Bij de scenario's 2 en 3 is de doorlooptijd aanzienlijk korter dan bij scenario 1 omdat hier van de bestaande radionetwerken van de mobiele operator(s) gebruik gemaakt wordt. Bij de inschatting van de doorlooptijd van de scenario's 2 en 3 is ervan uitgegaan dat de overheid niet kiest voor een volledig redundant transmissienetwerk. Voor deze redundantie zou in de scenario's 2 en 3 een extra doorlooptijd gelden van 1 tot 2 jaar. Bij scenario 1 wordt de doorlooptijd van de aanbesteding tot oplevering op 8-10 jaar; er moet een totaal nieuw mobiel breedbandnetwerk opgebouwd worden. Een onderdeel dat de doorlooptijd mede bepaalt, is de verwerving van nieuwe antenne opstelpunten.
- ***Internationaal***: De internationale ontwikkeling van het eco systemen van netwerkapparatuur en randapparatuur speelt een belangrijke rol. Er wordt in scenario 2 en 3 gebruik gemaakt van de frequenties van de massamarkt, te verwachten is dat apparatuurleveranciers voor deze frequenties kiezen. Scenario 3 scoort op het criterium *Internationaal* iets hoger dan scenario 2, omdat hier de overheid een eigen core heeft en de volledige controle over de koppelvlakken met externe (en internationale) netwerken. Het eigen netwerk en eigen spectrum van scenario 1 kunnen beperkingen geven in de internationale afstemming en ontwikkeling van het eco systeem.
- ***Migratie***: In scenario 2 wordt het beheer uitgevoerd door de operators waarbij operators ruime ervaring hebben met het migreren van grote zakelijke gebruikers. In de scenario's 1 en 3 zal de overheid naast het huidige C2000 ook delen van het nieuwe breedbandnetwerk beheren. Voor deze scenario's heeft de overheid een grotere verantwoordelijkheid en minder ervaring in het uitvoeren van de migratie.
- ***Risico's*****:** De risico's van scenario 2 en 3 zijn aanzienlijk lager dan bij scenario 1. Het bouwen van een volledig eigen netwerk brengt grote risico's met zich mee in de doorlooptijd, de kosten en het kennisniveau van de overheid.

De criteria waarop scenario 3 beter scoort zijn:

- ***Beveiliging***: Scenario 3 heeft op een aantal criteria een hogere score, wat met name heeft te maken met het feit dat de core in eigendom en eigen beheer is van de overheid zelf; de overheid kan dus zelf aanvullende maatregelen nemen bij de selectie van leveranciers en de beveiliging, zowel technisch als organisatorisch.
- ***Internationaal***: Scenario 3 scoort internationaal iets hoger omdat hier de overheid een eigen core heeft en de volledige controle over de koppelvlakken naar externe netwerken.

De criteria waarop scenario 1 beter scoort zijn:

- ***Beveiliging***: In Scenario 1 heeft de overheid de volledige (operationele) controle over de oplossing. Hierbij heeft het ook de controle over de beveiliging.

5.4 Resultaten Business Case

5.4.1 Financiële vergelijking scenario's

De financiële vergelijking van de drie toekomstscenario's is uitgewerkt in exploitatiekosten en investeringen. Voor dit financiële overzicht zijn uitgangspunten gekozen om een globale financiële vergelijking te kunnen maken tussen de drie toekomstscenario's.

We hebben hierbij als generiek uitgangspunt gekozen dat er altijd een optimum gekozen zal worden tussen de kosten en de missiekritische eisen. De maatregelen die de Nederlandse overheid eventueel kan nemen in de vorm van additionele wetgeving zijn in deze business case buiten beschouwing gelaten.

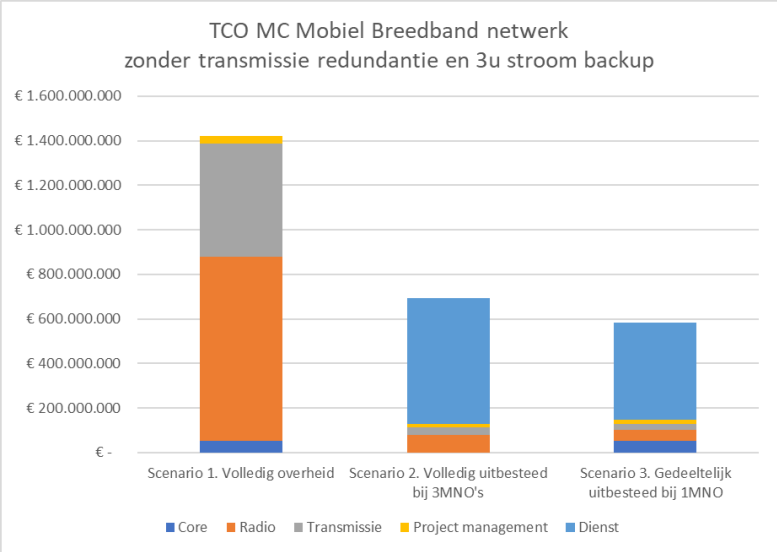
De algemene uitgangspunten voor de financiële vergelijking zijn:

- Deze financiële vergelijking is "high level" en gebaseerd op globale inschattingen en aannames zoals hieronder aangegeven;
- Doel van deze financiële vergelijking is om een eerste inzicht in de financiële consequenties te geven van de verschillende scenario's en deze onderling te vergelijken om zo de keuzerichting mede te kunnen bepalen;
- In een vervolgtraject moet een gedetailleerdere kostencalculatie (business case) gemaakt worden op nadere keuzes en uitgebreidere informatie.

Specifieke aannames en uitgangspunten zijn in onderstaande tabel opgenomen.

Uitgangspunten financiele vergelijking missie kritische mobiele breedband		
Onderdeel van de high level financiële vergelijking:		
• investeringskosten; core-; transmissie-; radionetwerk; projectmanagement		
• exploitatie en beheerkosten; core-; transmissie-; radionetwerk		
• kosten van operator diensten		
Scenario	Uitgangspunt	
1-2-3	Oplossing op basis van 4G technologie	
1-2-3	Contractstermijn	10 jaar
1-2-3	Aantal mobiele aansluitingen op netwerk	175.000
1	Aantal antenne locaties	2340
2-3	Uitbreiding antenne locaties	150-100
1	Gebruikt spectrum	700-3500MHz
2-3	Gebruikt spectrum	MNO-spectrum
1-3	Core en NOC redundant uitgevoerd	
2	Core en NOC	MNO
optioneel	redundantie in het transmissie netwerk	
optioneel	stroomuitval overbrugging 3 uur -> 6 uur	
Niet meegenomen in de high level financiële vergelijking:		
• Verwervingskosten		
• Migratie kosten		
• Roaming kosten buitenland		
• Prive gebruik van zakelijke randapparatuur		
• Gebruikersbeheer		

De resultaten van de financiële vergelijking zijn in de onderstaande figuren weergegeven. De detailuitwerking van de financiële vergelijking is opgenomen in bijlagen A5.



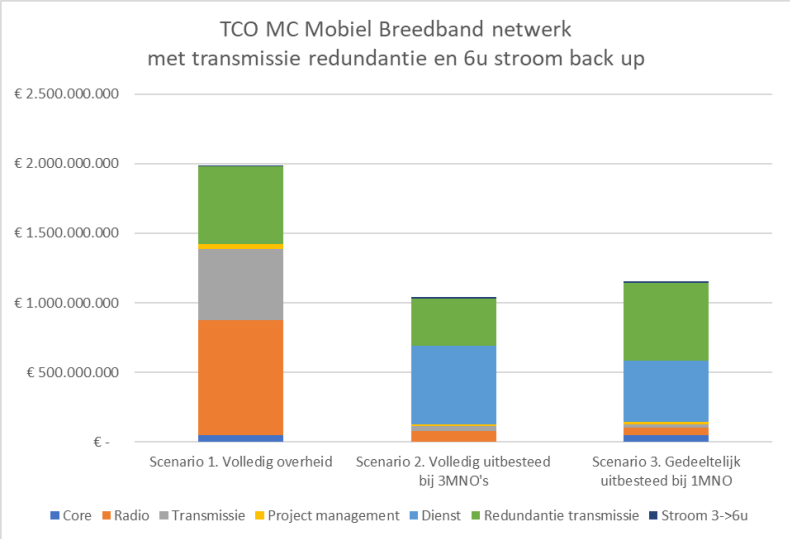
Figuur 21. Total cost of ownership scenario's zonder redundantie en 3 uur overbrugging stroomonderbreking

In de bovenstaande grafiek is de TCO (total cost of ownership) weergegeven op basis van de eenmalige investeringskosten en de jaarlijkse exploitatie kosten over de contractsperiode van 10 jaar. De verschillende kleuren geven de kosten per netwerkonderdeel aan: core-netwerk, radionetwerk, transmissienetwerk, projectmanagement en operatordiensten. Optionele zaken als transmissie netwerk redundantie via gescheiden paden en langere stroomuitval overbruggingstijd dan drie uur zijn niet meegenomen.

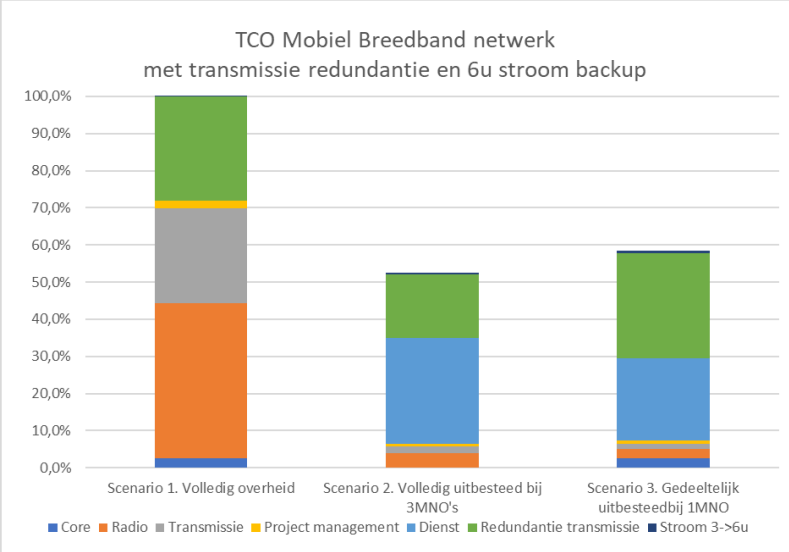
De kosten van scenario 1 zijn ongeveer tweemaal hoger dan de kosten van scenario 2. Scenario 3 scoort ongeveer 16% lager in kosten dan scenario 2. Dit zijn vooral de extra kosten doordat alle drie de operators worden gecontracteerd, wat meer capaciteit, redundantie en dekking geeft, maar ook overlap in drie overeenkomsten.

Wat verder opvalt, is dat in scenario 1 het radionetwerk en het transmissienetwerk hoge kosten met zich meebrengen, samen namelijk 93%. In dit scenario zijn de kosten van het core-netwerk relatief laag; 4% van de totale kosten.

Indien de optionele functies worden meegenomen in de financiële vergelijking (transmissieredundantie in groen en zes uur stroomuitval overbruggingstijd in donkerblauw), dan zijn de kosten van de drie scenario's zoals in de navolgende figuren weergegeven.



Figuur 22. Total cost of ownership scenario's met redundantie en 6 uur overbrugging stroomonderbreking

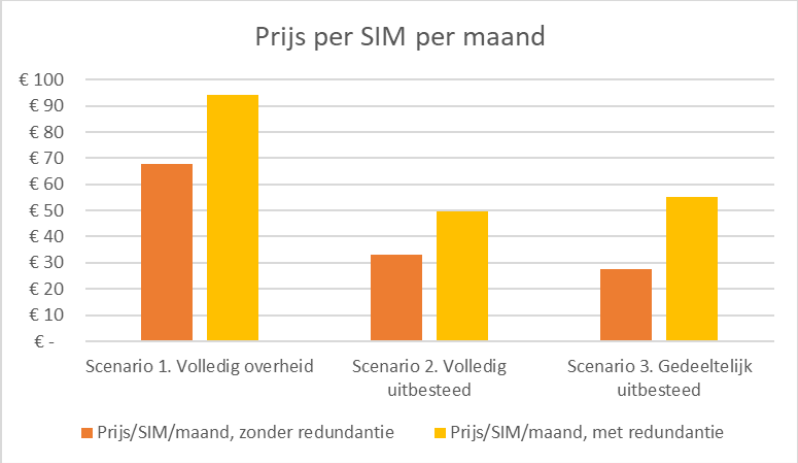


Figuur 23. Total cost of ownership scenario's met redundantie procentueel

De TCO (total cost of ownership) wordt hiermee aanzienlijk hoger (28% voor scenario 1) omdat in veel gevallen nieuwe verbindingen naar de antenne-opstellocaties aangebracht moeten worden om de benodigde redundantie te kunnen realiseren.

De kosten van scenario 2 zijn 53% van de kosten van scenario 1. Scenario 3 wordt in deze berekening naar verhouding duurder omdat in scenario 2 een deel van de redundantie wordt gerealiseerd door gebruik te maken van de radio-netwerken van de drie operators waardoor al een deel van de redundantie standaard aanwezig is. Scenario 3 wordt nu ongeveer 11% duurder dan scenario 2.

In de navolgende grafiek zijn de kosten per SIM per maand weergegeven voor de drie scenario's. Hiermee vergelijken we de kosten per gebruiker in de situaties met en zonder extra redundantie.

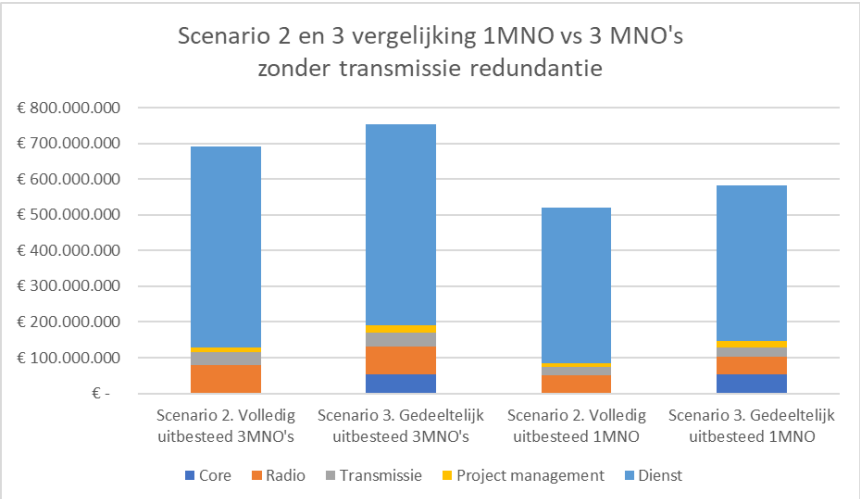


Figuur 24. Prijs per SIM per maand

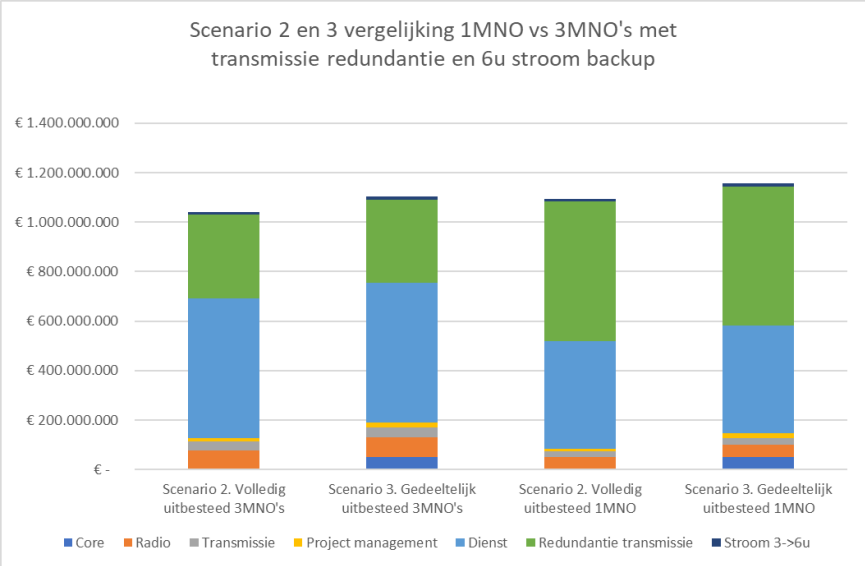
De kosten per SIM per maand voor een missiekritische mobiele breedbandoplossing zijn aanzienlijk hoger dan de huidige tarieven in de mobiele zakelijke markt voor een SIM zonder specifieke kwaliteitsgaranties (deze kosten zijn op dit moment voor veel overheidsorganisaties rond de €4,-/SIM/maand).

5.4.2 Detailvergelijking scenario 2 en scenario 3

Tussen scenario 2 en scenario 3 zijn er twee variabelen onderscheidend, namelijk het core-netwerk (uitbesteed aan de operator of overheid eigen) en het aantal MNO's (één of drie). Om een nadere analyse te kunnen doen op het financiële onderscheid van deze variabelen hebben we in de onderstaande figuren scenario 2 en 3 met elkaar vergeleken met één MNO en met drie MNO's.



Figuur 25. Scenario 2 en 3 vergelijking met één MNO en drie MNO's zonder redundantie



Figuur 26. Scenario 2 en 3 vergelijking met één MNO en drie MNO's met redundantie

Voor de scenario vergelijking van met drie MNO's zonder redundantie heeft scenario 2 9% lagere kosten dan scenario 3. De kosten van het core-netwerk zijn in scenario 3 met drie MNO's zonder redundantie 7%.

Voor de scenario vergelijking van met één MNO zonder redundantie heeft scenario 2 12% lagere kosten dan scenario 3. De kosten van het core-netwerk zijn in scenario 3 met één MNO zonder redundantie 9%.

Het kostenverschil voor één MNO of drie MNO's zonder redundantie is aanzienlijk, bij scenario 2 25% en bij scenario 3 is dit 23%.

Voor de scenariovergelijking met drie MNO's met redundantie heeft scenario 2 6,0% lagere kosten dan scenario 3. De kosten van het core-netwerk zijn in scenario 3 met drie MNO's met redundantie 4,7%.

Voor de scenariovergelijking van met één MNO met redundantie heeft scenario 2 5,7% lagere kosten dan scenario 3. De kosten van het core-netwerk zijn in scenario 3 met één MNO zonder redundantie 4,5%.

Bij de vergelijking één MNO versus drie MNO's met redundantie is de redundantie met één MNO naar verhouding duurder omdat met drie MNO's een deel van de redundantie wordt gerealiseerd door gebruik te maken van de radionetwerken van de drie operators waardoor al een deel van de redundantie standaard aanwezig is.

Indien transmissie-redundantie een vereiste is, is er een klein verschil (5%) in kosten tussen de scenario's met één MNO en drie MNO's (dit geldt zowel voor scenario 2 als 3). Het extra voordeel bij drie MNO's, dat er naast transmissie-redundantie ook radionetwerk-redundantie aanwezig is, is dan mogelijk tegen relatief beperkte kosten.

De kosten van een overheid eigen separaat core-netwerk is op de totale kosten van scenario 3 beperkt afhankelijk van de gekozen varianten één of drie MNO's en wel of geen redundantie, van 4,5 tot 9% van de totale kosten van het betreffende scenario.

5.4.3 Baten en kosten-baten afwegingen

In dit haalbaarheidsonderzoek is met name een globale vergelijking gemaakt van de kostenkant van de financiën.

Er zijn diverse variabelen die in de oplossingsrichtingen gekozen kunnen worden, echter deze hebben in veel gevallen ook kostenconsequenties. Voor een totale en gedetailleerde business case zullen ook de baten en de noodzaak van de gestelde eisen worden gewogen tegen de kosten. Zie hiervoor ook paragraaf 5.7.

Het is verstandig om eerst een scenariokeuze te maken op hoofdlijnen en vervolgens dat scenario in detail uit te werken inclusief een complete business case.

5.5 Voor- en nadelen per scenario

5.5.1 Voor- en nadelen per scenario

De voor- en nadelen van de drie onderzoeksscenario's zijn in deze paragraaf op hoofdlijnen per onderzoeksscenario weergegeven. Tevens zijn de voor- en nadelen van de huidige situatie weergegeven. Daarnaast zijn de mogelijkheden om de financiën in de business case te beïnvloeden per scenario aangegeven. Ten slotte geven we per scenario aan wat de belangrijkste risico's zijn plus eventuele maatregelen om deze risico's te mitigeren.

5.5.1.1 Scenario. 1 Volledig overheid

Voordelen van scenario 1:

+ De overheid heeft de volledige (operationele) controle over de oplossing; de overheid kan zelf de leveranciers van de verschillende componenten selecteren op basis van eigen criteria.
+ Het biedt de kans op een schaalbaar overheidsnetwerk (qua capaciteit en frequentiegebruik) waar andere overheidspartijen (ook op een later moment nog) op kunnen aansluiten.
+ Beveiliging in hoge mate in eigen hand.
+ Maakt gebruik van de standaarden van de massamarkt van 3GPP en biedt de mogelijkheid van open, leverancier-onafhankelijke oplossingen. Er zijn door 3GPP missiekritische standaarden ontwikkeld.
+ Doordat van 3GPP breedband technologie gebruik gemaakt wordt, kunnen naast spraak en korte databerichten ook breedband data- en videotoepassingen missie kritisch gebruikt worden.
+ Goed ecosysteem van netwerkcomponenten met meerdere leveranciers ten aanzien van de massamarkt-implementaties.

Nadelen van scenario 1:

- Deze oplossing is aanzienlijk duurder dan de andere oplossingen. Naar verwachting is deze oplossing ongeveer 100% duurder dan scenario 2, een volledig uitbestede dienst.
- De realisatietijd van de volledige overheidsoplossing is aanzienlijk langer dan wanneer de overheid de oplossing uitbesteedt. Met name de realisatie van een volledig mobiel breedband radionetwerk met een optimale radiodekking kost naar verwachting 4-6 jaar méér doorlooptijd dan een uitbestede oplossing.
- Voor een volledig overheidsnetwerk is specifiek radiospectrum noodzakelijk. Spectrum is zeer schaars en is op dit moment nog niet voldoende beschikbaar. Om dit scenario haalbaar te maken dient het ministerie van EZK additioneel frequentiespectrum beschikbaar te stellen. Voor een missiekritisch mobiel breedband-netwerk is voor calamiteitssituatie een aanzienlijke extra hoeveelheid spectrum noodzakelijk ten opzichte van de normale operatie. Hierdoor wordt er geen efficiënt gebruik gemaakt van schaars radiospectrum.
- De verwachting is dat het ecosysteem van mobiele devices zich bij het gebruik van eigen frequenties minder goed zal ontwikkelen dan bij het gebruik van standaard MNO-frequenties. Overigens is dit wel afhankelijk van de exacte frequenties die in dit scenario door het ministerie van EZK aan het ministerie van JenV zouden worden toegewezen.

5.5.1.2 Scenario 2 Volledig uitbesteed

Voordelen van scenario 2

+ De overheid is flexibeler in het op- en afschalen van de missiekritische mobiele dienstverlening, zowel in kosten als in de snelheid waarmee dat kan plaats vinden.
+ Aanzienlijk lagere kosten dan scenario 1 en vergelijkbaar met de kosten van scenario 3.
+ De radiodekking van deze oplossing is potentieel beter dan die van scenario 3 en mogelijk ook beter dan de dekking van scenario 1. Het radionetwerk van alledrie de MNO's van Nederland wordt gebruikt waardoor al een goede basisdekking wordt bereikt.
+ De telecommunicatiemarkt wordt in dit scenario niet verstoord, omdat aan de drie MNO's volgens gelijke randvoorwaarden wordt gevraagd diensten te leveren. Uiteraard zal mogelijk één van de drie een betere positie verkrijgen als die het core-netwerk levert en beheert.
+ Goede beveiliging van de oplossing is mogelijk, maar voor deze beveiliging is de overheid vrijwel volledig afhankelijk van toeleveranciers en de MNO's.
+ De realisatie tijd van deze oplossing is aanzienlijk korter dan die van scenario 1 en ook naar verwachting ook korter dan die bij scenario 3.
+ Het schaarse radiospectrum wordt efficiënt gebruikt omdat er gebruik gemaakt wordt van bestaand MNO-spectrum. Daarnaast zou het reeds beschikbare OOV-spectrum door operators in het MNO netwerk ingezet kunnen worden, waarbij buiten piekmomenten het ingezet kan worden voor andere klanten en doelen.
+ Maakt gebruik van de standaarden van de massamarkt van 3GPP biedt de mogelijkheid van open, leveranciersonafhankelijke, oplossingen. Er zijn door 3GPP missiekritische standaarden ontwikkeld.
+ Doordat van 3GPP breedband technologie gebruik gemaakt wordt, kunnen naast spraak en korte databerichten ook breedband data- en videotoepassingen missiekritisch gebruikt worden.
+ Goed ecosysteem van netwerkcomponenten en randapparatuur met meerdere leveranciers ten aanzien van de massamarkt implementaties. De verwachting is dat het ecosysteem van mobiele devices zich met bestaande MNO-frequenties beter zal ontwikkelen dan met eigen frequenties.

Nadelen van scenario 2

- De overheid heeft een heel beperkte controle over de oplossing, doordat alle netwerkcomponenten inclusief het beheer zijn uitbesteed aan toeleveranciers. Ten aanzien van beveiliging is het voor de overheid niet mogelijk om de volledige (operationele) controle bij toeleveranciers af te dwingen. Dit wordt voor een belangrijk deel veroorzaakt door het gegeven dat de overheid geen eigen core-netwerk heeft in dit scenario.
- De radionetwerken van alle MNO's in Nederland moeten worden aangepast op missiekritische eigenschappen.
- Het gebruik van de netwerken van alle MNO's maakt deze oplossing technisch en organisatorisch complexer.

5.5.1.3 Scenario 3 Gedeeltelijk uitbesteed

Voordelen van scenario 3:

+ De overheid is flexibeler in het op- en afschalen van missiekritische mobiele dienstverlening dan in scenario 1 het geval is, zij het licht minder flexibel dan in scenario 2.
+ Dit scenario kent aanzienlijk lagere kosten dan scenario 1 en is vergelijkbaar met de kosten van scenario 2.
+ Het radionetwerk van deze oplossing wordt geleverd als dienst door één MNO en is minder complex dan in scenario 2.

+ Goede beveiliging van de oplossing is mogelijk. De belangrijkste beveiligingscomponent in het mobiele breedbandnetwerk, het core-netwerk, heeft de overheid zelf onder controle. De overheid kan zelf de selectie doen van de toeleveranciers van de core-componenten. Voor het radionetwerk is de overheid afhankelijk van toeleveranciers, de MNO's.
+ De realisatie tijd van deze oplossing is aanzienlijk korter dan die van scenario 1, maar naar verwachting iets langer dan bij scenario 2.
+ Het schaarse radiospectrum wordt efficiënt gebruikt omdat er gebruik gemaakt wordt van bestaand MNO-spectrum. Daarnaast zou het reeds beschikbare OOV-spectrum door de operator in het MNO-netwerk ingezet kunnen worden, waarbij buiten piekmomenten het ingezet kan worden voor andere klanten en doelen.
+ Maakt gebruik van de standaarden van de massamarkt van 3GPP en biedt de mogelijkheid van open, leveranciersonafhankelijke oplossingen. Er zijn door 3 GPP missiekritische standaarden ontwikkeld.
+ Doordat van 3GPP-breedbandtechnologie gebruik gemaakt wordt, kunnen naast spraak en korte data-berichten ook breedband data- en videotoepassingen missiekritisch gebruikt worden.
+ Goed ecosysteem van netwerkcomponenten en randapparatuur met meerdere leveranciers ten aanzien van de massamarkt implementaties. De verwachting is dat het ecosysteem van mobiele devices zich met bestaande MNO-frequenties beter zal ontwikkelen dan met eigen frequenties.

Nadelen van scenario 3:

- De overheid heeft een beperkte controle over de oplossing. Ze heeft wel een aanzienlijk betere controle over de oplossing in vergelijking met scenario 2, omdat het core-netwerk in eigendom bij de overheid is. Maar ze heeft een beperktere controle ten opzichte van scenario 1, omdat het radionetwerk is uitbesteed bij één MNO.
- De radiodekking van deze oplossing is potentieel minder goed dan scenario 2. Door het inzetten van het radionetwerk van één MNO is er per definitie enigszins minder dekking en een beperktere redundantie in het radionetwerk.

5.5.1.4 Scenario 0 Huidige situatie C2000 en standaard mobiel breedband van operators

Het scenario 0 is de huidige situatie met als missiekritisch netwerk C2000, dit is geen mobiele breedband oplossing. Naast het gebruik van C2000 maken alle OOV-organisaties op dit moment gebruik van de publieke mobiele breedbanddiensten die de Nederlandse mobiele operators op de markt aanbieden. Deze diensten zijn echter "best effort" en geen missiekritische oplossing. Scenario 0 geldt in dit onderzoek als referentie scenario.

Voordelen van scenario 0:

+ C2000 is inmiddels een bewezen oplossing qua technologie, implementatie en gebruik.
+ Bij C2000 heeft de overheid volledige controle over de oplossing. Dat geldt niet voor de publieke breedbanddiensten waar de overheid ook gebruik van maakt.
+ De gebruikers van C2000 zijn gewend aan deze oplossing en zijn voorganger (sinds 2004 operationeel en in januari 2020 is het netwerk vervangen).
+ C2000 heeft een goede beveiliging.
+ C2000 is volledig ingebed in de werkprocessen van alle gebruikers.
+ De mobiele breedband diensten van operators worden toegepast. Deze diensten werken onder normale omstandigheden redelijk tot goed en hebben een relatief laag kostenniveau.

Nadelen van het 0-scenario:

- C2000 is geen breedbandoplossing en is niet toekomstvast. De oplossing is alleen geschikt voor spraaktoepassing en korte databerichten. De oplossing is niet geschikt voor breedbandige data- en videotoepassingen.
- C2000 is geen open oplossing en er is slechts beperkte standaardisatie. Voorbeelden: Bij TETRA is alleen de air interface gestandaardiseerd. Om smalbandige TETRA-netwerken onderling te kunnen koppelen wordt gebruik gemaakt van een zeer complexe interface. Hierdoor zijn er in de praktijk zeer weinig TETRA-netwerken onderling gekoppeld (alleen in Scandinavië is dit gerealiseerd). De meldkamer-interface is vanuit TETRA niet gestandaardiseerd.
- Voor C2000 is een beperkt ecosysteem van slechts enkele leveranciers die veelal leveranciersgebonden gesloten (additionele) oplossingen ontwikkeld hebben. Dit geldt ook voor randapparatuur.
- C2000 maakt gebruik van verouderde technologie.
- De huidige mobiele breedband oplossingen van de mobiele operators bieden geen garanties op bijvoorbeeld kwaliteit, radiodekking, beschikbaarheid, performance. Ze zijn niet op basis van missiekritisch eisen ingekocht. Er is bij deze diensten een aanzienlijk tot groot risico dat onder missiekritisch omstandigheden (rampen, grote incidenten) de huidige mobiele breedband diensten niet of zeer beperkt beschikbaar zijn.

5.6 Risico's

5.6.1 Risico's algemeen

In deze paragraaf zijn de belangrijkste risico's voor een nieuwe mobiele breedband oplossing voor missiekritische toepassing opgenomen. De risico's zijn ingedeeld in algemene risico's die op alle scenario's van toepassing zijn en specifieke risico's per scenario. Per risico is aangegeven welke maatregelen genomen kunnen worden om het betreffende risico te mitigeren. In veel gevallen brengt het mitigeren van de risico's kosten met zich mee. Daarnaast blijft er in veel gevallen nog een restrisico over waarvan het de vraag is of de overheid bereid is om dit te accepteren.

Algemene risico's die voor alle scenario's gelden:

Risico's algemeen	**Maatregel**
De huidige door 3GPP gestandaardiseerde MC-spraakfunctionaliteit is voor de gebruikers in Nederland niet toereikend. De 3GPP-standaarden zijn niet in alle gevallen volledig vergelijkbaar met de TETRA-oplossing (bijvoorbeeld de DMO, direct mode operation) functie. Dit kan inhouden dat gebruikers in mobiel breedband niet kunnen beschikken over exact dezelfde functionaliteit als in TETRA.	De verwachting is dat het gebruik van missiekritische datatoepassingen de behoefte aan spraaktoepassingen zal wijzigen. Nader onderzoeken wat de (detail)verschillen zijn tussen TETRA en MC-PTT (spraak) en of deze verschillen gecompenseerd worden door de nieuwe datatoepassingen.
De beveiligingsoplossing van 3GPP wordt door de Nederlandse overheid als onvoldoende veilig beoordeeld voor missiekritische toepassingen.	Additionele beveiligingsmaatregelen kunnen toegevoegd worden op applicatieniveau om de beveiliging naar een voldoende niveau te verhogen.
De overheid wordt afhankelijk voor de oplossing van (toe)leveranciers.	Bij de verwerving voorkomen dat er een vendor lock-in kan ontstaan door te zorgen voor een modulaire opzet, gebruik van standaarden en goede exitclausules

De overheid heeft geen ervaring met de verwerving en operatie van een missiekritisch mobiel breedband-netwerk/-dienst.	1. Maximaal leren van landen die voor hetzelfde oplossingsscenario gekozen hebben en in de implementatie hiervan verder zijn dan Nederland. 2. De overheid vergaart kennis bij ervaren partijen in de markt en laat de eigen medewerkers trainen. 3. Waar mogelijk gemengde teams inzetten van eigen medewerkers en medewerkers van de leveranciers om zo de eigen medewerkers ervaring en kennis op te laten doen.
Ecosysteem. Er is op dit moment nog geen groot ecosysteem van oplossingen die volledig voldoen aan de meest relevante missiekritische standaarden (MCX) van 3GPP omdat dit nog in ontwikkeling is. Dit geldt zowel voor toepassingen als voor randapparatuur. De verwachting is dat het ecosysteem zich zal ontwikkelen, maar dat dit nog enkele jaren nodig heeft. Het is onzeker of dit ecosysteem volledig op open standaarden gebaseerd gaat worden.	Door internationaal te oriënteren wat andere (grotere) landen gaan doen, kan Nederland aansluiten bij de ontwikkeling van internationale ecosystemen. Voor de randapparatuur is het van belang de spectrumkeuze af te stemmen op wat in de markt gangbare frequenties zijn die door randapparatuur ondersteund worden. Dit is ook van belang om de Nederlandse randapparatuur te laten functioneren op buitenlandse missiekritische mobiele netwerken.
De overheid stelt te hoge eisen aan een missiekritische mobiele breedband oplossing waardoor die in de praktijk niet realiseerbaar.	1. De eisen van de Nederlandse overheid vroegtijdig toetsen aan de eisen van landen die al over zijn gegaan op aanbesteding en/of implementatie. Hiermee kan kennis en ervaring van andere landen gebruikt worden bij het bepalen van de randvoorwaarden en eisen. 2. Het uitvoeren van een goede marktconsultatie om inzicht te verkrijgen in wat wel en niet mogelijk is, als basis voor een programma van eisen bij aanbesteding.
De oplossingen voor missiekritische breedbandtoepassingen zijn in veel gevallen nog niet volledig in de praktijk bewezen (field proven). Hoe lang duurt het nog voordat de oplossing field proven is? Zeker in vergelijking met de huidige TETRA-technologie die door de jarenlange ervaring wel bewezen is.	Met name bij het toepassen van MCX over 5G-technologie gaat het field proven nog wel enige tijd duren (tot na 2024 is de verwachting). Indien Nederland eerder gebruik wil maken van missiekritische mobiele breedband zou dit risico verlaagd kunnen worden door te starten op MCX over 4G-technologie en pas later over te stappen naar 5G-technologie.
De doorlooptijd van de implementatie wordt sterk beïnvloed door de verwerving van de nieuwe radio-opstelpunten; gemiddeld duurt de verwerving van een nieuw opstelpunt twee jaar.	1. Onderzoeken of bij de opstelpunten volledig van de bestaande C2000-opstelpunten gebruik gemaakt kan worden. 2. Speciale verordening afkondigen om het verwervingsproces te versnellen. Dit zal bij lokale overheden mogelijk weerstand oproepen. Daarnaast is

	er ook verzet te verwachten in verband met de inspraakprocedure van bewoners. 3. Uitwerken van adequate site-sharing afspraken met de MNO's.

5.6.2 Risico's per scenario

5.6.2.1 Risico's van scenario 1 en mogelijkheden om de risico's te mitigeren

Risico's scenario 1.	**Maatregel**
De algemene risico's (zie hierboven)	
Er is onvoldoende frequentiespectrum beschikbaar bij de start en gedurende de levensduur van het netwerk doordat het gebruik van missiekritische toepassingen sterker groeit dan verwacht. Zonder de beschikking over voldoende spectrum is dit scenario niet haalbaar	Bij de start voldoende spectrum vrijmaken voor een eigen netwerkoplossing. De hoeveelheid spectrum moet gebaseerd zijn op de te verwachten pieksituaties. Het frequentiespectrum zal gedurende de looptijd van deze oplossing naar behoefte uitgebreid moeten kunnen worden via de BOP-procedure. Hier zullen maatregelen vanuit de overheid noodzakelijk zijn om in deze behoefteontwikkeling te kunnen blijven voorzien.
Aan een complex project met zeer lange looptijd en grote investeringen kleeft het risico om het resultaat niet binnen de gestelde tijd en het beschikbare budget te bereiken. Na de implementatie is het risico dat de overheid het (complexe) beheer niet onder controle krijgt. Het is de vraag of de overheid een dergelijk complex project gecontroleerd kan uitvoeren.	De overheid is eigenaar van het netwerk maar besteedt de opbouw en operatie van het netwerk uit aan een specialist in de markt. Aan deze specialist worden dan specifieke beveiligingseisen gesteld om de beveiliging op het vereiste niveau te krijgen. Dit doet echter mogelijk afbreuk aan het uitgangspunt waarbij de overheid de volledige controle heeft over het netwerk.
Er wordt in de oplossing geen efficiënt gebruik gemaakt van frequentiespectrum.	1. De basisbehoefte van de hulpdiensten wordt ingevuld met eigen spectrum. Voor de piekbehoefte wordt gebruik gemaakt van MNO-radionetwerken en dus ook MNO-spectrum. Dit doet echter afbreuk aan het uitgangspunt waarbij de overheid de volledige controle heeft over het netwerk. 2. Vraagbundeling toepassen waardoor meerdere overheidsdiensten voor hun missiekritische toepassingen gebruik maken van de beschikbare capaciteit. Let wel, ook dit kan marktverstorend werken; die partijen hebben immers hun huidige dienstverlening veelal nu ook gewoon bij MNO's ondergebracht.

5.6.2.2 *Risico's van scenario 2 en mogelijkheden om de risico's te mitigeren*

Risico's scenario 2.	**Maatregel**
De algemene risico's (zie hierboven)	
De overheid is voor de beveiliging volledig afhankelijk van MNO's en diens toeleveranciers.	Het beveiligingsniveau van de oplossing vergroten door eisen te stellen aan de MNO-organisatie die de dienst gaat leveren. Bijvoorbeeld door te eisen dat deze organisatie volledig separaat moet zijn met specifieke beveiligingsniveaus die afgestemd zijn op de behoefte van de overheid. Deze maatregel zal kostenverhogend werken.
Het netwerk van (1 of meer) mobiele operators voldoet niet aan de capaciteits-, beschikbaarheids- of andere eisen van de overheid.	De operators (1 of meer) passen hun netwerken aan zodat zij wel kunnen voldoen en de overheid is bereid om de kosten hiervoor te betalen. De gebruiksvoorwaarden van het frequentiespectrum voor de operators aanpassen. Accepteren dat bij de oplossing van dit scenario niet van het netwerk van 3 operators wordt gebruik gemaakt maar van minder operators. Indien er geen operator kan voldoen en ook er geen bereidheid is om aanpassingen door te voeren, zoeken naar alternatieven die met concessies tot een optimum leiden.

5.6.2.3 *Risico's van scenario 3 en mogelijkheden om de risico's te mitigeren*

Risico's scenario 3	**Maatregel**
De algemene risico's (zie hierboven)	
De overheid is voor de beveiliging gedeeltelijk afhankelijk van toeleveranciers.	Het beveiligingsniveau van de oplossing vergroten door specifieke beveiligingseisen te stellen aan de MNO-organisatie die de radiodekkingsdienst gaat leveren.
De overheid heeft geen ervaring met inrichten van en het uitvoeren van het beheer van een mobiel breed-band core-netwerk.	1. De overheid richt het beheer in naar voorbeeld van ervaren partijen in de markt (zoals MNO's) en laat de medewerkers die het operationeel beheer moeten uitvoeren, trainen door deze ervaren partijen. 2. De overheid is eigenaar van het core-netwerk maar besteedt de opbouw en operatie van het netwerk uit aan een specialist in de markt. Aan deze specialist worden dan specifieke beveiligingseisen gesteld om de beveiliging op het vereiste niveau te krijgen. Dit doet

	echter afbreuk aan het uitgangspunt waarbij de overheid de controle heeft over het core-netwerk. Dit kan initieel worden ondervangen door een volledig separate core te eisen en op termijn de operator te vervangen door een eigen, interne beheerorganisatie.
Het netwerk van (1 of meer) mobiele operators voldoet niet aan de capaciteits-, beschikbaarheids- of andere eisen van de overheid.	De geselecteerde operator past zijn netwerk aan zodat het netwerk wel voldoet en de overheid is bereid om de kosten hiervoor te betalen. Indien er geen operator kan voldoen en er ook geen bereidheid is om aanpassingen door te voeren, moet er gezocht worden naar alternatieven die met concessies tot een optimum leiden.
Er is een risico dat de telecommunicatiemarkt wordt verstoord doordat gebruik gemaakt wordt van het (radio)netwerk van slechts één MNO. Deze MNO zal (delen van) het radionetwerk missiekritisch maken en hiermee de beschikbaarheid en kwaliteit verhogen en de radiodekking vergroten, gefinancierd met overheidsgeld. Dit kan een significant effect hebben op de concurrentiepositie van deze MNO in de massamarkt.	In plaats van één MNO selecteren, de missiekritische dienst baseren op de diensten van alledrie de MNO's, en de te investeren verbeteringen verdelen over alle de de MNO's. Indien 1 MNO geselecteerd wordt en in het netwerk van deze MNO geïnvesteerd gaat worden, zorgen dat dit geen concurrentievoordeel gaat bieden Indien 1 MNO geselecteerd wordt en in het netwerk van deze MNO geïnvesteerd gaat worden, zorgen dat de andere 2 gecompenseerd worden.

5.7 Mogelijkheden om de financiën te beïnvloeden

5.7.1 Algemeen

De mogelijkheden om de financiën te beïnvloeden zijn gesplitst in mogelijkheden die voor alle scenario's gelden en mogelijkheden per scenario.

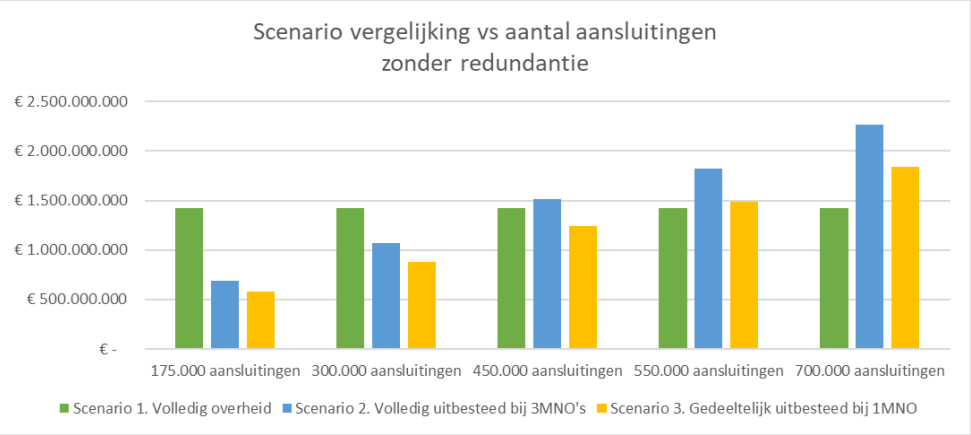
Voor alle scenario's gelden de volgende mogelijkheden om de financiën te beïnvloeden:

- Afwegingen maken van de noodzaak van gestelde eisen versus de financiële consequenties. Bijvoorbeeld het realiseren van redundantie in het transmissienetwerk, via gescheiden routes, heeft een verhoging van de kosten tot gevolg van ongeveer 30% in alledrie de scenario's. Door een afweging te maken van de risico's met de kans dat een verstoring voor komt en de impact ervan, en vervolgens te zoeken naar alternatieve oplossingen, kan een lager kostenniveau worden bereikt.
- De looptijd van het contract verlengen waardoor afschrijvingen op investeringen over een langere periode kunnen plaats vinden.
- Schaalvergroting, door de behoefte van andere overheidsorganisaties te bundelen met de behoefte van het ministerie van JenV. Hierbij kan met meer inkoopvolume een grotere inkoopkracht opgebouwd worden en de additionele investeringen die MNO's moeten doen worden over een grotere groep gebruikers verdeeld.

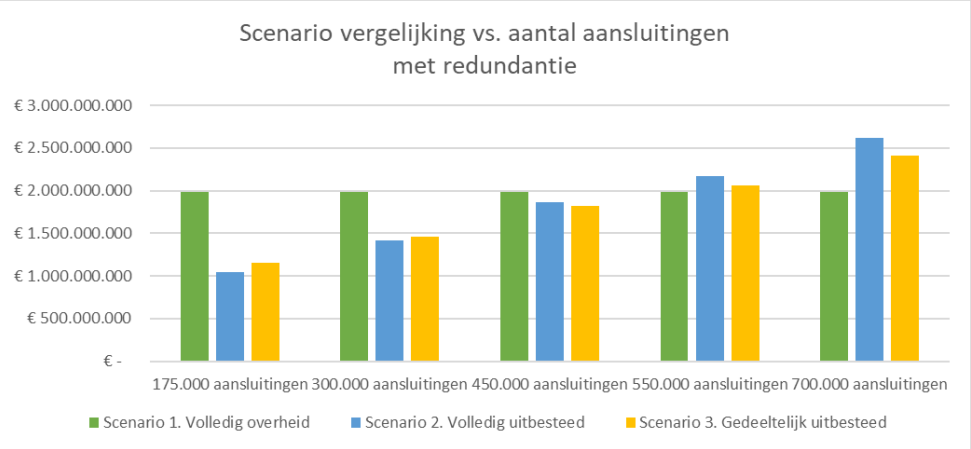
5.7.2 *Per scenario*

5.7.2.1 *Mogelijkheden om de financiën te beïnvloeden voor scenario 1:*

- Schaalvergroting, door de behoefte van andere overheidsorganisaties, ten behoeve van publieke taken, te bundelen met de behoefte van het ministerie van JenV (175.000 aansluitingen) kunnen meerdere organisaties gebruik maken van deze overheidsinfrastructuur. Voor een relatief klein land als Nederland met relatief veel inwoners is het verschil tussen een eigen overheidsnetwerk of volledig uitbesteden vanuit business case oogpunt substantieel. Het scenario zou toch overwogen kunnen worden bij het bundelen van de overheidsbehoefte aan kritische communicatie.
  In onderstaande figuur worden van de scenario's de break-even punten aangegeven voor een oplossing met redundantie in het transmissie netwerk (bij 500.000 aansluitingen) en zonder redundantie in het transmissie netwerk (bij 400.000 aansluitingen). Indien het aantal gebruikers in plaats van 175.000 op 500.000 komt te liggen, is er een financiële basis om dit scenario verder te onderzoeken.



Figuur 27. Scenario vergelijking versus aantal aansluitingen zonder redundantie



Figuur 28. Scenario vergelijking versus aantal aansluitingen met redundantie

- Voor de inkoop van de netwerkcomponenten meeliften op de inkoopkracht van (internationale) MNO's.
- Onderzoeken of bij de antenne opstelpunten volledig van de bestaande C2000-opstelpunten gebruik gemaakt kan worden.
- De redundantie van deze oplossing zoeken buiten de oplossing, door bijvoorbeeld de fall-back te laten verzorgen door een MNO. Dit doet echter afbreuk aan het uitgangspunt waarbij de overheid de volledige controle heeft over het netwerk.

5.7.2.2 Mogelijkheden om de financiën te beïnvloeden voor scenario 2:

- De redundantie van deze oplossing realiseren bij twee MNO's in plaats van bij alledrie de MNO's. Dit leidt tot een optimalisatie van de kosten voor redundantie over twee in plaats van drie partijen.
- Het spectrum in de 700MHz-band (2x3+2x5=2x8MHz bandbreedte) dat gereserveerd is voor OOV-organisaties kan ingebracht worden in de aanbesteding waarbij MNO's deze frequenties mogen gebruiken voor hun massadienstverlening, maar de OOV-organisaties krijgen prioriteit (op alle frequenties) indien noodzakelijk. Internationaal wordt dit bijvoorbeeld in de Verenigde Staten met FirstNet al toegepast.

5.7.2.3 Mogelijkheden om de financiën te beïnvloeden voor scenario 3:

- De redundantie van deze oplossing zoeken bij de twee of drie MNO's in plaats van bij één MNO.
- Het spectrum in de 700MHz-band (2x3+2x5=2x8MHz bandbreedte) dat gereserveerd is voor OOV-organisaties, kan ingebracht worden in de aanbesteding waarbij MNO's deze frequenties mogen gebruiken voor hun massadienstverlening, maar de OOV-organisaties krijgen prioriteit indien noodzakelijk. Internationaal wordt dit bijvoorbeeld in de Verenigde Staten met FirstNet al toegepast.

6 CONCLUSIES

6.1 Algemene conclusie ten aanzien van de haalbaarheid

De hoofdvraag van dit haalbaarheidsonderzoek is: kan de Nederlandse overheid op een verantwoorde manier missiekritische communicatie realiseren over een mobiel breedbandnetwerk?

Vanuit de 3GPP-organisatie wordt nog volop gewerkt aan de benodigde standaarden voor missiekritische communicatie. De huidige releases van de standaarden zijn gebaseerd op 4G omvatten veel maar nog niet de volle functionaliteit zoals die nu binnen C2000 beschikbaar is. Er zijn ook nog geen leveranciers die de 4G missiekritische standaarden volledig hebben geïmplementeerd. De 3GPP missiekritische standaarden voor 5G komen pas eind 2021 beschikbaar en kunnen daarna pas door leveranciers worden geïmplementeerd. De eerste implementaties zullen dan op zijn vroegst rond 2023-2024 beschikbaar komen. Om die reden is het antwoord op de hoofdvraag, dat het op dit moment te vroeg is om een absoluut bevestigend antwoord te geven. Tegelijkertijd geven de standaardisatieontwikkelingen voldoende aanleiding om te verwachten dat dit binnen enkele jaren wel zo zal zijn. Dat is een risico, maar gezien de snelheid waarmee dat wordt opgepakt en het gegeven dat vele andere landen ook gekozen hebben voor 3GPP-standaarden, zien wij op dit moment geen reden waarom de overheid zou moeten afwijken van de (voorlopige) richting zoals verwoord in de Tweede Kamer-brief van december 2019.

6.2 In eigen beheer of uitbesteden?

Missiekritische communicatie is van groot strategisch belang en vormt een essentiële én onmisbare voorziening voor de OOV-organisaties. Daarnaast ondersteunt het grote operationele- en nationale veiligheidsbelangen. De eerste vraag die daarbij voor een overheid naar voren komt, is die van uitbesteden of zelf doen. Scenario 1 van het onderzoek heeft als uitgangspunt, dat de overheid alles in eigen beheer uitvoert, zowel de inrichting als het beheer. Wat zijn de voor- en nadelen van ‘eigen beheer’?

Uit de analyse springen drie voordelen van eigen beheer in het oog:

- Maximale strategische en politieke invloed op de oplossing.
- Volledige zeggenschap over de beveiliging van de oplossing, binnen de kaders die de gekozen apparatuur biedt.
- Hogere mate van leveranciersonafhankelijkheid. De overheid heeft (binnen de grenzen van de aanbestedingswetgeving) de ruimte om zelf te bepalen op basis van welke technologie zij haar netwerk bouwt, welke leverancier(s) componenten mogen leveren en welke dienstverleners ze inhuurt. Let wel, ook in dit scenario blijft er voor de overheid een afhankelijkheid van leveranciers bestaan; volledig onafhankelijk zou alleen kunnen als de overheid zelfstandig de noodzakelijke apparatuur en software ontwikkelt en produceert. Dat is te complex, te kostbaar en onhaalbaar.

Uit de analyse kwamen meerdere nadelen naar voren:

- Er is nu onvoldoende spectrum gealloceerd in het Nationale Frequentieplan (NFP) voor een eigen overheidsnetwerk. Het is op dit moment vrijwel onmogelijk om genoeg aanvullend spectrum beschikbaar te krijgen omdat geschikt frequentiespectrum reeds toegewezen is aan andere partijen.
- Een eigen netwerk opbouwen vergt een langere doorlooptijd, met name om voldoende antenne-opstelpunten en transmissielijnen te realiseren.
- De overheid beschikt op dit moment niet over een eigen netwerkoperator voor breedbandnetwerken. Dat betekent dat alle kennis en personeel moet worden verworven in een markt waar deze mensen schaars zijn. Er is binnen de overheid wel kennis en ervaring met C2000 aanwezig, maar niet met mobiel breedband.

- Er zijn grote investeringen en operationele lasten gemoeid met dit scenario. De high level financiële vergelijking laat zien dat het grofweg tweemaal zo duur is als de scenario's van uitbesteden.

Een netwerk in eigen beheer levert dan wel meer invloed en zeggenschap op, maar vanwege het ontbreken van voldoende frequentieruimte, het ontbreken van eigen kennis en ervaring en de hoge kosten achten wij een mobiel breedbandnetwerk in eigen beheer (scenario 1) als drager voor missiekritische communicatie **niet haalbaar**.

In het buitenland zijn geen landen bekend waar al wel voor dit scenario is gekozen. Er lopen wel verkenningen bij diverse landen (o.a. Duitsland) om een basis breedbandvoorziening in overheidseigendom aan te gaan leggen. Onze verwachting is dat er in Europa vrijwel landen zijn, die een volledig eigen missiekritisch mobiel breedbandnetwerk zullen aanleggen, maar dat in alle gevallen een oplossing zal worden gebouwd met het radionetwerk van één of meer mobiele operators. In Duitsland is men voornemens om mogelijk wel een eigen basisvoorziening te realiseren, maar de piekcapaciteit te betrekken van commerciële operators. In het Verenigd Koninkrijk en Finland heeft de overheid besloten om een eigen core-netwerk aan te leggen en het VK heeft dit ook al gerealiseerd.

6.2.1 Uitbesteden

Als in eigen beheer opzetten van een missiekritische breedband communicatienetwerk niet haalbaar is, blijft de optie van uitbesteden over. Daarbij spelen de vragen *wat* en aan *wie* uitbesteed kan worden een rol. In het onderzoek hebben we de keuze *uitbesteden* als scenario 2 (volledig uitbesteden) en scenario 3 (gedeeltelijk uitbesteden met eigen core) onderzocht.

Een mobiel breedbandnetwerk bestaat simpel gesteld uit een radionetwerk, een transmissienetwerk en een core-netwerk. Bij de aanleg van een mobiel breedbandnetwerk zijn de grootste investeringen gemoeid met de opbouw van het radionetwerk en het aanleggen van het transmissienetwerk. Door het grote aantal benodigde antenne-opstelpunten en de fysieke graaf- en installatiewerkzaamheden vergt de aanleg van het radionetwerk en het transmissienetwerk ook nog eens vele jaren. Daarnaast is veel doorlooptijd gemoeid met het verkrijgen van de benodigde (lokale) vergunningen.

De oplossing ligt in het g*edeeld gebruik* van het radionetwerk en het transmissienetwerk. In de publieke markt voor mobiele communicatie zijn veel van dergelijke 'MVNO[18]' samenwerkingsvormen bekend waarbij mobiele operators gebruik maken van de netwerkvoorzieningen van andere operators. Het ligt dan ook voor de hand om het radionetwerk en het transmissienetwerk uit te besteden aan één of meerdere MNO's.

Relevant in deze afweging zijn de veiligheidseisen die de overheid stelt aan een missiekritisch breedbandnetwerk. Op dit moment zijn deze eisen nog niet gespecificeerd. Op basis van de eisen kan bepaald worden of de overheid essentiële delen (zoals het core-netwerk) in eigen beheer moet nemen of dat ook deze uitbesteed mogen worden.

In het onderzoek zijn twee uitbesteed-scenario's (2 en 3) onderzocht: alles uitbesteden en gebruik maken van drie radionetwerken van mobiele operators (scenario 2) of alleen het radionetwerk en de transmissie uitbesteden bij één mobiele operator en het core-netwerk komt in eigendom van de overheid (scenario 3).

[18] MVNO staat voor Mobile Virtual Network Operator; operators die geen eigen radionetwerk hebben en in veel gevallen ook geen core netwerk, provisioning- en billing systeem hebben maar daarvoor gebruik maken van het netwerk en systemen van een MNO. De MVNO heeft een eigen marketing, klanten en een klantenservice. Bekende voorbeelden op de Nederlandse consumentenmarkt zijn Simpel, AH, Lebara, Hollandse Nieuwe, etc.

Scenario 2 heeft als voordeel dat de overheid in veel mindere mate eigen technische en operationele expertise hoeft te verwerven en dat meegelift kan worden op de bestaande infrastructuren van de huidige MNO's. Dat verkort de doorlooptijd t.o.v. scenario 1 met enkele jaren. Door aan te sluiten op de radionetwerken van alle MNO's wordt extra redundantie in het radionetwerk verkregen, is er potentieel een grotere capaciteit bij calamiteiten beschikbaar (dit vergt nadere afspraken over prioriteit van verkeer) en is er aldus een betere beschikbaarheid. Voor de beveiliging is de overheid afhankelijk van de keuzen die de operators maken en de mogelijkheid om aanvullende afspraken te maken.

Scenario 3 biedt voordelen op het punt van zeggenschap, onafhankelijkheid en beveiliging omdat het core-netwerk in eigendom en beheer van de overheid is. De kosten van het core-netwerk zijn relatief laag in vergelijking met de kosten van het totale netwerk. Uit de financiële vergelijking komt naar voren dat het core-netwerk ongeveer 4% van de totale kosten van een compleet mobiel breedbandnetwerk vertegenwoordigt. Voor deze relatief lage kosten krijgt de overheid een aanzienlijke controle over het totale netwerk.

6.2.1.1 Zeggenschap in geval van uitbesteden

In december 2019 is een Algemene Maatregel van Bestuur "Besluit veiligheid en integriteit telecommunicatie" in werking getreden die de regering de mogelijkheid geeft om telecomdienstverleners te verbieden om netwerkapparatuur en/of -diensten van bepaalde leveranciers te gebruiken, in geval via deze leveranciers andere landen invloed uitoefenen op telecomvoorzieningen in Nederland. Hiermee heeft de overheid een vergaande mogelijkheid om in te grijpen. Het is echter de vraag is of deze maatregel toereikend is.

Of de juridische mogelijkheid die met deze AMvB is gecreëerd is, de belangen van de missiekritische diensten voldoende kan beschermen kan pas worden vastgesteld als de eisen (met voorop de veiligheids- en beschikbaarheidseisen) helemaal helder zijn. De verwachting is, dat deze eisen hoger zullen liggen dan de eisen die aan generiek gebruik, zoals de publieke, commerciële massamarkt, worden gesteld.

De AMvB heeft betrekking op aanbieders van *openbare* elektronische communicatienetwerken ook als deze worden ingezet voor missiekritische diensten. Het is de vraag of de AMvB toereikende bescherming biedt voor de missiekritische breedbanddiensten of dat aanvullende maatregelen noodzakelijk zijn.

De operators zijn volop bezig met de inrichting van hun 5G-netwerken zonder dat er, op basis van de genoemde AMvB, nu leveranciers zijn uitgesloten. Of de MNO's al voorsorteren op een mogelijke uitsluiting van een of meerdere leveranciers, is ons niet bekend. Dat betekent dat als er op een later moment een leverancier wordt uitgesloten waarvan al componenten zijn opgenomen in de 5G-netwerken, de operator de betreffende componenten moet vervangen door componenten van een andere leverancier. Dit zal tot forse desinvesteringen leiden, waarvoor de operator bij de overheid zal aankloppen voor nadeelcompensatie.

Het is dan ook onzeker of de mobiele operators tegemoet willen en kunnen komen aan de (nog te specificeren) eisen. Die eisen zullen in veel gevallen naast de additionele kosten ook een langere doorlooptijd tot gevolg hebben.

6.2.2 Afweging tussen onderzochte scenario's

Zowel scenario 2 als scenario 3 scoren hoog in de uitgevoerde multi-criteria analyse, waarbij scenario 2, *Volledig uitbesteed*, een iets hogere score heeft gekregen. Dat komt omdat op de meeste aspecten waar een verschil is tussen de scenario's 2 en 3, met uitzondering van beveiliging, dit in het voordeel uitvalt van scenario 2. Zie de onderstaande figuur voor de scores per criterium.

Behoefte	Weging	Scenario 1: Volledig Overheid		Scenario 2: Volledig Uitbesteed		Scenario 3: Gedeeltelijk Uitbesteed		0-Scenario: Huidige C2000-oplossing	
	1-3	Punten	Gewogen	Punten	Gewogen	Punten	Gewogen	Punten	Gewogen
1. Strategisch / politiek	1	77,5	77,5	52,5	52,5	72,5	72,5	57,5	57,5
2. Techniek	3	78,8	236,3	80	240	76,3	228,8	62,5	187,5
3. Beveiliging	3	85	255	60	180	67,5	202,5	65	195
4. Innovatie en toekomstvastheid	1	90	90	90	90	90	90	0	0
5. Frequentie spectrum	3	0	0	100	300	100	300	93,8	281,3
6. Organisatie	3	25	75	75	225	50	150	37,5	112,5
8. Besturing	2	70	140	70	140	70	140	40	80
9. Juridisch	1	92,5	92,5	100	100	85	85	95	95
10. Tijd / planning	2	20	40	75	150	75	150	25	50
11. Internationaal	3	50	150	90	270	95	285	5	15
12. Migratie	2	50	100	90	180	75	150	45	90
13. Risico's	3	12,5	37,5	81,3	243,8	56,3	168,8	18,8	56,3
Totaal	**27**	**651,3**	**1293,8**	**963,8**	**2171,3**	**912,5**	**2022,5**	**545**	**1220**
Relatieve score tov beste:		**60%**		**100%**		**93%**		**Dit is geen breedband-oplossing**	
Relatieve score tov max:		**48%**		**80%**		**75%**			
Rang:		**3**		**1**		**2**			

Figuur 29. Totaaloverzicht resultaten multicriteria-analyse

Met de hoogste score voor scenario 2 is niet gezegd, dat dit ook het te realiseren scenario moet zijn. Zoals in paragraaf 2.2 bij de keuze voor de drie scenario's is aangegeven, geeft dit onderzoek inzicht in de *haalbaarheid* en de eigenschappen van het gebruik van op 3GPP gebaseerd mobiele breedbandtechnologie en is het niet gericht op het selecteren van het optimale scenario.

Uit de analyse komt ook een nieuwe variant naar voren, waarbij uitbesteden aan meerdere operators gecombineerd wordt met de inrichting van een 'eigen' core-netwerk ('scenario 3a'). Dit core-netwerk kan volledig in eigen beheer, zoals in de scenario's 1 en 3, maar er bestaat ook een uitbestedingsvariant; hierbij richt de operator voor de overheid, separaat van zijn eigen core-netwerk, een missiekritisch core-netwerk in. Door zowel fysiek als logisch een geheel losstaande core in te richten, beheerd door een afgescheiden beheerteam, verkrijgt de overheid alsnog de maximale controle over zowel de beveiliging als de functionaliteit van de core.

Om een definitieve afweging tussen de scenario's en eventuele tussenliggende varianten te kunnen maken moeten in de komende periode verschillende verdiepingsslagen gemaakt worden. Reeds genoemd is het nader uitwerken van de beveiligingseisen; in het hoofdstuk 7. Aanbevelingen geven we aan op welke andere punten nog onderzoek gepleegd moet worden. De uitkomst van de verdiepingsslagen bepaalt of bepaalde criteria zwaarder of juist lichter moeten wegen, of dat aanvullende maatregelen nodig zijn om een scenario te kunnen realiseren.

In het bepalen van de 'routekaart' voor de komende jaren speelt de in het begin van dit hoofdstuk al genoemde standaardisatie-ontwikkeling een belangrijke rol. Het risico dat de markt niet tijdig de vanuit missiekritische toepassingen gewenste releases aanbiedt, kan beperkt worden door het huidige C2000-netwerk parallel naast de missiekritische mobiele breedbandoplossing (in ontwikkeling) operationeel te houden. Indien gebruik gemaakt wordt van het radionetwerk van mobiele operators kan de mobiele breedbandoplossing gefaseerd ingericht worden. Daarbij wordt de routekaart bepaald door de 3GPP-releaseontwikkeling (4G-5G-6G) en kunnen de kosten beperkt worden door de eisen af te stemmen op het actuele gebruik qua omvang, capaciteit en van niet- naar missiekritisch.

In de afweging moet ook het risico meegenomen worden dat Nederland een afwijkende koers volgt ten opzichte van andere landen. Het aantal gebruikers van missiekritische communicatie is relatief klein ten opzichte van de totale markt voor mobiele breedbandcommunicatie. Afwijkende eisen en/of specificaties kunnen leiden tot een oneven-redig hogere prijs, of de beslissing van een MNO om de dienst niet aan te gaan bieden. Ook kan het de operationele samenwerking met OOV-organisaties uit andere landen ernstig bemoeilijken. Ook vanuit het perspectief van de MNO's die in meerdere landen actief zijn, is het zeer wenselijk dat de eisen in alle landen waar ze actief zijn, zoveel mogelijk gelijk zijn. Het is daarom ook verstandig om constant te kijken naar de keuzes (en consequenties daarvan) die in andere landen worden gemaakt, waar mogelijk aan te sluiten bij standaarden en best practices en daarnaast te leren van de consequenties van gemaakte keuzes door anderen landen die 'voorop' lopen, zoals bijvoorbeeld het Verenigd Koninkrijk en Finland.

7 AANBEVELINGEN

Op basis van de resultaten van dit haalbaarheidsonderzoek hebben we de volgende aanbevelingen:

1. Bepaal op basis van de behoefteontwikkeling voor missiekritische communicatie de **uitgangspunten** voor het missiekritische mobiel breedband netwerk inclusief de **benodigde netwerkcapaciteit op detail niveau**. Houdt bij deze capaciteit rekening met gemiddeld gebruik en piekgebruik.

2. **Onderzoek de mogelijkheden en wensen van medeoverheden om vraagbundeling** toe te passen om zo het aantal gebruikers van een missiekritisch communicatienetwerk te vergroten. Een groter aantal gebruikers leidt tot lagere variabele kosten en vergroot de aantrekkelijkheid voor MNO's. Hierbij kan gedacht worden aan partijen als Rijkswaterstaat, Prorail, de huidige gelieerde gebruikers etc.

3. Stel op basis van de beveiligingseisen een **high level definitiestudie** op, om het concept van de technische architectuur van een missiekritische communicatievoorziening op basis van de uitbestedingsscenario's te toetsen. Tevens zal een analyse gemaakt moeten worden of de missie kritische oplossing op basis van 4G dan wel op 5G technologie gerealiseerd gaat worden. Verder zal een meer gedetailleerde invulling van het core-netwerk moeten worden bepaald (geen eigen core, core in eigen beheer of eigen core beheerd door een operator). Het MVNE (mobile virtual network enabler) architectuurmodel biedt de mogelijkheid om een operator neutraal core netwerk te koppelen met de radionetwerken van meerdere operators op basis van de zogenoemde MOCN (multi-operator core-netwerk) interfaces of op basis van S8 roaming interfaces.

4. Zet met leveranciers en mede-overheden **proeftuinen** op om te verifiëren dat de functionaliteit van MCX-diensten van leveranciers of MNOs onder verschillende omstandigheden op voldoende niveau functioneert.

5. Houd na afloop van de aankomende frequentieveiling **een nieuwe marktconsultatie met de Nederlandse operators**. De marktconsultatie heeft als doel om de bereidheid te polsen van operators om missiekritische communicatiediensten aan te gaan bieden o.b.v. de 3GPP-standaarden en om de technische, operationele, commerciële en juridische (on)mogelijkheden, condities en randvoorwaarden te verkennen van de aansluiting van een eigen core op de radionetwerken van de drie operators. Onderzoek met de MNO's wat een haalbare *worst case* noodzakelijke capaciteit is (aan de celranden) van de mobiele netwerken van de operators. De marktconsultatie kan gebruikt worden om te verkennen op welke wijze de operators geholpen kunnen worden om de uitrol te versnellen. Hierbij denken we onder meer aan het openstellen van bestaande C2000-antenne-opstelpunten aan meerdere operators, en het inbrengen van het specifieke spectrum in de 700MHz-band dat in het frequentieplan is gealloceerd voor OOV-gebruik.

6. Stel op korte termijn de **beveiligingseisen voor missiekritische communicatie** op en betrek hierbij ook de expertise en risico-analyse capaciteiten van relevante overheidsdiensten als NCTV, NCSC en AIVD. Deze eisen zijn sterk bepalend voor de definitieve scenariokeuze en de daarbinnen te kiezen varianten.

7. Bepaal in overleg met wetgevingsjuristen de exacte **werking van de AMvB** om te bepalen of deze afdoende bescherming biedt tegen dreigingen van statelijke actoren. Voer overleg met de MNO's om de consequenties te bespreken.

8. Voer na een verdere concretisering van de voorkeursoplossingsrichting een **gedetailleerde risicoanalyse** uit.

9. Werk in meerdere iteratiestappen een **business case** uit die inzicht geeft in de vereiste investeringen en operationele kosten. Aanbevolen wordt om de business case mede te gebruiken om tot een detailafweging van een programma van eisen te komen, zodat meer inzicht wordt gekregen in de financiële consequenties van elke eis of wens.

10. **Onderzoek of de in het buitenland gehanteerde wijzen van financiering** interessant zijn voor de Nederlandse situatie. Een voorbeeld is Finland waar de dienst wordt bekostigd vanuit een maximumbedrag per SIM per maand.

11. **Neem actief deel aan internationale ontwikkelingen** en met name aan de EU-initiatieven zoals BroadWay en BroadNet. Nederland is niet het enige land die voor de keuze staat om een opvolger te selecteren voor missiekritische netwerken. Het is aan te bevelen dat Nederland zeer actief de internationale ontwikkelingen volgt en actief participeert in de standaardisatiegremia. Samen optrekken met buurlanden ligt vanuit operationele samenwerking van OOV-organisaties voor de hand. Nederland kan het beste aansluiten bij de keuzes van het internationale collectief (landen met vergelijkbare uitgangspunten als Nederland). Naast kennis- en inkoopvoordelen, levert dit ook een bijdrage aan het te ontwikkelen ecosysteem. Belangrijke keuzes zijn hierbij:

    - De 3GPP-standaarden en welke specifieke release.
    - Het frequentiespectrum dat gebruikt gaat worden. Dit is van belang voor de internationale samenwerking waarbij missiekritische organisaties bij grensoverschrijdende activiteiten van elkaars netwerken gebruik gaan maken. Het is ook van belang voor het in voldoende mate beschikbaar zijn van de benodigde randapparatuur afkomstig van diverse leveranciers.
    - Afstemmen met de buitenlandse missiekritische organisaties ten aanzien van frequentiegebruik en de eisen aan randapparatuur om ervoor te zorgen dat de randapparatuur die door Nederland geselecteerd wordt ook internationaal kan functioneren.
    - Kennisontwikkeling; met de kennis en ervaring die internationaal is opgedaan kan Nederland op basis van de lessons learned risico's afdekken.
    - Nederland wil aansluiten met het Nederlandse missiekritische breedbandnetwerk op het Europese BroadNet en zal daarbij moeten voldoen aan de nog op te stellen aansluitvoorwaarden van BroadNet.

12. **Start de voorbereiding van het verwervingsproces.** Nadat de oplossingsrichting is vastgesteld en de marktconsultatie met de MNO's heeft plaatsgevonden, kan de aanbestedingsstrategie worden ontwikkeld. Afhankelijk van de realisatieplanning en de beschikbaarheid van de missiekritische functies in 5G zal er een keuze gemaakt moeten worden of de oplossing start op basis van 4G-technologie met een migratie naar 5G of dat direct 5G-technologie zal worden toegepast.

13. In alle scenario's heeft de overheid eigen **kennis nodig van mobiele breedbandnetwerken en -diensten** op een niveau waarop zij dat nu nog niet heeft. Begin daarom vroegtijdig met het verkrijgen van toegang tot de benodigde kennis en borg deze kennis. In alle scenario's, dus ook als gekozen wordt voor uitbesteden, is het noodzakelijk om strategische netwerkkennis in huis te hebben op het gebied van de standaarden, architectuur, beveiliging en configuratie. Een eerste stap is om aan de hand van het meest waarschijnlijke scenario en de planning na te gaan op welk moment welke aanvullende behoefte er is ten opzichte van de huidige aanwezige kennis. Bundel vervolgens alle reeds beschikbare expertise.

Bijlagen

A.1 Definities en verklaring afkortingen

Afkorting	Verklaring	Website
3GPP	3rd Generation Partnership Project	www.3gpp.org
4G	Vierde generatie mobiele netwerken ook wel LTE genoemd	www.3gpp.org
5G	Vijfde generatie mobiele netwerken	www.3gpp.org
AIVD	Algemene Inlichting- en Veiligheidsdienst, onderdeel van het ministerie van binnenlandse zaken	www.aivd.nl
AMvB	Algemene Maatregel van Bestuur, besluit van de regering, wettelijke regels nader uitgewerkt. Voor telecommunicatienetwerken is er in november 2019 een AMvB vastgesteld. Zie: https://zoek.officielebekendmakingen.nl/stb-2019-457.html	www.rijksoverheid.nl
APCO-25	ook wel P-25 genoemd, Amerikaanse standaard voor missie kritische smalband communicatie	
BDBOS	De overheidsorganisatie in Duitsland die het missie kritische mobiele netwerk beheert	www.bdbos.bund.de
BIT	Bureau ICT Toetsing	www.bureauicttoetsing.nl
BroadMap	EU initiatief waarin de missie kritische breedband behoefte is gespecificeerd	www.broadmap.eu
BroadNet	EU initiatief waarin op termijn de UE missie kritische breedband oplossing wordt gerealiseerd	www.broadway-info.eu
BroadWay	EU initiatief waarin de UE missie kritische breedband oplossing wordt ontwikkeld	www.broadway-info.eu
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	www.rijksoverheid.nl

C2000	Huidige missiekritische mobiele netwerk in Nederland	
DGP&V	Directoraat Generaal Politie en Veiligheidsregios, onderdeel ministerie JenV	www.rijksoverheid.nl
DJI	Dienst Justitiële Inrichtingen	
DL	DownLink, de verbinding van het mobiele netwerk naar het mobiele device	www.3gpp.org
DMO	Direct Mode Operation; een back up functie in TETRA indien het netwerk uitgevallen is.	
ESMCP	Emergency Services Mobile Communications Program, organisatie die ESN in de VK realiseert	www.gov.uk
ESN	Emergency Services Network, missie kritisch breedband netwerk in het Verenigd Koninkrijk	www.gov.uk
ETSI	European Telecommunications Standards Institute	www.etsi.org
EU	Europese Unie	www.europa.eu
EZK	Ministerie van Economische Zaken en Klimaat	www.rijksoverheid.nl
FLEX	Proprietary standaard (Motorola) voor paging. In Nederland wordt het Flex protocol gebruikt voor P2000 alarmering.	
FirstNet	Het missiekritische mobiel breedbandnetwerk in de Verenigde Staten	www.firstnet.com; www.firstnet.gov
GSM-R	GSM-rail (Global System for Mobile communications ook wel 2G genoemd)	www.3gpp.org
HSS	Home Subscriber Server, onderdeel van mobiel breedband core netwerk	www.3gpp.org
IenW	Ministerie van Infrastructuur en Waterstaat	www.rijksoverheid.nl

IPA	Infrastructure and Project Authority, organisatie in het VK dat complexe overheidsprojecten controleert	www.gov.uk
IPsec	Internet Protocol Security is een standaard voor het beveiligen van het Internetprotocol door middel van encryptie.	
IVC	Implementatie Vernieuwing C2000	
JenV	Ministerie van Justitie en Veiligheid	www.rijksoverheid.nl
LTE	Long Term Evolution, naam voor mobiel netwerk ook wel 4G genoemd	www.3gpp.org
MAM	Mobile Application Management tool	
MC	Mission Critical	www.3gpp.org
MCX	Mission Critical Spraak, Data en Video	www.3gpp.org
MDM	Mobile Device Management tool	
MHz	Mega Hertz, eenheid van frequentie	
MME	Mobility Management Entity, onderdeel van mobiel breedband core netwerk	www.3gpp.org
MNO	Mobile Network Operator	www.gsma.com
MOCN	Multi-operator core-netwerk, interface mogelijkheid in mobiel core netwerk	www.3gpp.org
MVNE	Mobile Virtual Network Enabler, op een operator onafhankelijk core netwerk kunnen meerdere radionetwerken van operators aangesloten worden en er kunnen meerdere MVNO's gecreëerd worden voor separate gebruikersgroepen.	
MVNO	Mobile Virtual Network Operator, een mobiele operator zonder eigen radio netwerk	

NCSC	National Cyber Security Centrum	www.ncsc.nl
NCTV	Nationaal Coordinator Terrorismebestrijding en Veiligheid	www.nvtv.nl
NFP	Nationaal Frequentie Plan	www.agentschaptelecom.nl
Nødnett	De benaming van het missie kritische netwerk in Noorwegen	www.nodnett.no
OOV	Openbare Orde en Veiligheidsdiensten	
P2000	Onderdeel van C2000, het paging of alarmeringsnetwerk gebaseerd op de FLEX standaard	
P25	Project 25, Amerikaanse standaard voor missie kritische smalband communicatie	
PCP	Pre-Commercial Procurement, ontwikkelingsprogramma in samenwerking met de markt	
PCRF	Policy and Charging Rules Function, onderdeel van mobiel breedband core netwerk	www.3gpp.org
PCStorm	Ontwikkelprogramma voor missie kritische breedband in Frankrijk	
P-GW	Packet Gateway, onderdeel van mobiel breedband core netwerk	www.3gpp.org
ProSe	Proximity-based Services; binnen 3GPP gestandaardiseerde fall back service indien het breedband network uitgevallen is. Er zijn echter nog geen oplossingen in de markt die vergelijkbaar zijn met DMO bij TETRA	
PSCE	Public Safety Communications Europe	www.psc-europe.eu
RAN	Radio Access Netwerk, het antenne netwerk in een mobiel netwerk	www.3gpp.org

S8	De 3GPP S8 roaming interface wordt toegepast om de mobiele netwerken van verschillende mobiele operators te koppelen.	
SA WG6	3GPP werkgroep die zich bezich houdt met de standaardisatie van missiekritische functies	www.3gpp.org
SCL	Special Coverage Location, locatie waar binnenhuis dekking voor missie kritische communicatie vereist is	
S-GW	Serving Gateway, onderdeel van mobiel breedband core netwerk	www.3gpp.org
SIM	Subscriber Identity Module, onderdeel in het mobiele device dat zorgt voor de authenticatie op een mobiel netwerk	www.3gpp.org
Strict	Strict, de onderzoekers	www.strict.nl
SUCI	SUbscription Concealed Identifier. Methode om in een 5G netwerk de identiteit van een gebruiker te versleutelen.	www.3gpp.org
T2000	Onderdeel van C2000, het portofoon netwerk gebaseerd op de TETRA standaard	
TCCA	The Critical Communications Association, belangen organisatie van leveranciers en gebruikers	www.tcca.info
TEDS	TETRA Enhanced Data Services	www.etsi.org
TETRA	Terrestrial Trunked Radio, de ETSI standaard voor digitale missie kritische smalband communicatie	www.etsi.org
TETRAPOL	Proprietary standaard (Matra, EADS, Airbus) voor digitale missie kritische smalband communicatie	
TK	Tweede Kamer	www.detweedekamer.nl
UL	UpLink, de verbinding van het mobiele device naar het mobiele netwerk	www.3gpp.org

Virve	De benaming van het missie kritische netwerk in Finland	www.erillisverkot.fi
VKA	Verdonck, Klooster & Associates, de onderzoekers	www.vka.nl
WBI	Werkgroep Bijzondere Informatiebeveiliging	www.rijksoverheid.nl

A.2 Bron informatie

Nr.	Naam Brondocument	Bestandsnaam brondocument	Auteur brondocument	Datum (brondoc.)
1.	Offerteaanvraag 1	Offerteaanvraag haalbaarheidsonderzoek Strict.pdf	Ministerie van Justitie en Veiligheid	18-12-2019
2.	Offerteaanvraag 2	10100035446 Offerteaanvraag Uitvoeren haalbaarheidsonderzoek opvolger C2000 versie 1.0.pdf	Ministerie van Justitie en Veiligheid	7-2-2020
3.	Plan van Aanpak Strict/VKA	PvA (W1) Min JenV 202001-5687 R2 V3.docx	Strict/VKA	14-2-2020
4.	Monitor Draadloze Technologie 2019	TNO-2019-R11692_Monitor_Draadloze_Technologie_Najaar_2019.pdf	TNO	1-11-2019
5.	Next-Gen Emergency Networks 2018	Analysys Mason Cost Model 25-07-2018.pdf	Analysys Mason	18-7-2018
6.	PPDR Roadmap	january-2019-ppdr-broadband-roadmap.pdf	TCCA	1-5-2019
7.	StaVaZa Min J&V TK Opvolger C2000	tk-stand-van-zaken-verkenning-opvolger-c2000.pdf	Ministerie van Justitie en Veiligheid	12-11-2019
8.	Bijl. 1 Vergunning 700MhZ	703-733MHz en 758-788 MHz ten behoeve van het aanbieden van elektronische communicatiediensten (Bijl1).pdf	Agentschap Telecom	25-11-2019
9.	Bijl. 3 Vergunning 1900-2100MhZ	0-1980 MHz en 2110-2170 MHz ten behoeve van het aanbieden van elektronische communicatiediensten (Bijl3).pdf	Agentschap Telecom	25-11-2019
10.	Bijl. 5 Transitievergunning 1900-2100MhZ	0-1980 MHz en 2110-2170 MHz ten behoeve van het aanbieden van	Agentschap Telecom	25-11-2019

		elektronische communicatiediensten (Bijl5).pdf		
11.	TETRA & LTE compared	2016-August_P3_Comparing_TETRA_DMO_with_-LTE_ProSe.pdf	TCCA/P3	1-8-2016
12.	Brief Stas TK Frequentie en Nationale Veiligheid	Brief Stas aan TK december_2019,_over_mogelijke_spionage_door_Huawei_in_Nederland_en_de_veiling_van_5G-frequenties.pdf	Staatssecretaris EZK	3-2-2020
13.	Cybersecurity 5G Networks	Cybersecurity_of_5G_networks_EU_Toolbox_of_risk_mitigating_measures.pdf	NIS Cooperation Group	1-1-2020
14.	Brief MinJ&V TK Cybersecuritybeeld Nederland 2019	Cybersecuritybeeld_Nederland_2019_(CSBN_2019)_en_voortgangsrapportage_NCSA_.pdf	Ministerie van Justitie en Veiligheid	12-6-2019
15.	Cybersecuritybeeld NL 2019	Cybersecuritybeeld_Nederland_CSBN_2019.pdf	Nat. Coördinator Terrorismebestrijding en Veiligheid	1-6-2019
16.	Stas EZK Ontwerp Capregeling Frequenties	d frequentieruimte voor mobiele communicatie (Capregeling frequenties mobiele communicatie 2020).pdf	Staatssecretaris EZK	-
17.	McKinsey Connected World discussion paper	MGI_Connected-World_Discussion-paper_February-2020.pdf	McKinsey Global Institute	1-2-2020
18.	McKinsey Connected World executive summary	MGI_Connected-World_Executive-summary_February-2020.pdf	McKinsey Global Institute	1-2-2020
19.	NCTS Weerbare vitale infrastructuur	NCSC - Factsheet+Weerbare+Vitale+Infrastructuur+NL+2018.pdf	Nat. Coördinator Terrorismebestrijding en Veiligheid	1-12-2017
20.	Radiocom. objectives and requirements for PPDR	R-REP-M.2377-1-2017-MSW-E.docx	International Telecommunication Union	1-11-2017

21.	Ontwerp besluit Veiling 700, 1400 en 2100 MHz	Ontwerp_van_het_Besluit_bekendmaking_veiling_vergunningen_700,_1400_en_2100_MHz.pdf	Staatssecretaris EZK	-
22.	Bijl. 2 Vergunning 1452-1492MhZ	Bijlage 2. band 1452-1492 MHz ten behoeve van het aanbieden van elektronische communicatiediensten.pdf	Staatssecretaris EZK	25-11-2019
23.	Bijl. 4 Toelichting Vergunningen	Toelichting_vergunningen_700,_1400,_2100_MHz-veiling.pdf	Staatssecretaris EZK	25-11-2019
24.	Ontwerp Regeling Frequentievaststelling	Regeling aanvraag- en veilingprocedure vergunningen 700, 1400 en 2100 MHz.pdf	Staatssecretaris EZK	-
25.	Brief Stas TK Frequentiebeleid	van de consultatie van de regelgeving inzake de veiling van de 700, 1400 en 2100 MHz-frequenties.pdf	Staatssecretaris EZK	5-12-2019
26.	Brief Stas TK Nationale Veiligheid	Vaststelling_AMvB_Besluit_veiligheid_en_integriteit_telecommunicatie.pdf	Staatssecretaris EZK	27-11-2019
27.	Brief Stas TK Nationale Veiligheid ontwerp AMVB	Vertrouwelijke ter inzage legging AMvB Besluit veiligheid en integriteit telecommunicatie.pdf	Staatssecretaris EZK	26-11-2019
28.	Voortgang NCSA	Voortgang_Nederlandse_Cybersecurity_Agenda.pdf	Onbekend	-
29.	Stratix Cost elements Rollout 5G Networks	Onderzoek+naar+de+kosten+van+5G-uitrol+(English).pdf	Stratix	5-4-2018
30.	Mission critical implementations tested during the 4th ETSI MCX PLUGTESTS	ETSI MCx plugtesten resultaten 30-09-2019.pdf	ETSI	30-9-2019
31.	Introduction to Mission Critical service interoperability	January-2020-Introduction-to-Mission-Critical-Service-Interoperability.pdf	TCCA	jan-20

32.	A public agency roadmap for successful MC PTT implementation	WP-Public-Safety-Agency-Roadmap-for-Successful-MCPTT-Implementation_PSN	The Public Satefy Network LLC (USA)	apr-20
33.	Plugtests scenarios for Mission Critical Services	ts_103564v010201p plugtest 2019	ETSI	mrt-19
34.	Review of the UK Public Account Committee on ESN	Emergency Services Network PAC rapport juli 2019	PAC (UK)	jul-19
35.	Stratix Spectrum efficiency voor overheids breedband netwerk	Breedband voor OOV-sector in de 700MHz band	Stratix	feb-17
36.	Facilitering missie-kritisch mobiel breedband voor het OOV-domein	TNO-2017-R11193	TNO	20-10-2017
37.	Alternatives for mission critical services in public mobile networks in Norway	20180503-conceptual-models-for-ngn-v1.0	DSB Norway	3-5-2018
38.	Virve 2.0 RfI responses	WP_Virve_2_0_RFI_2018_responses_-_Copy	Virve	2018
39.	Pan-European interoperable broadband Broadway PCP	TD1 RFT EN	Broadway	15-2-2019
40.	What is Virve 2.0?	fact_sheet_Virve_ENG_140319_-_Copy	Virve	mrt-2019
41.	FirstNEt Voorbeeld nieuwsbrief	March FirstNet Newsletter	FirstNet	mrt-2020
42.	A Broadband Strategy for German Critical Communications	barbara-held-a-broadband-strategy-foe-german-critical-communications	DBBos	mrt-2019

43.	France's PC Storm critical broadband project moves forward	PC Storm France 2019-05-02	PC Storm	2-5-2019
44.	Min JenV presentatie STRICT mei 2019	Min JenV presentatie STRICT.pdf	Strict	22-5-2019
45.	TNO Mobiel Breedband voor OOV 2018	Mobiel Breedband voor OOV Presentatie TNO.pdf	TNO	2018
46.	Q&A's verkenning opvolger C2000	Q&A's verkenning opvolger C2000.docx	Dimitri Gilissen	begin 2020
47.	FirstNet Roadmap 2019	20190813 FirstNet_Roadmap.pdf	FirstNet	13-8-2019
48.	3GPP release planning 5G	20200211 3GPP release planning 5G.pdf	3GPP	11-2-2020
49.	Kickoff meeting Onderzoeksteam	20200303 Kickoff meeting.pdf	Strict/VKA	3-3-2020
50.	Kamerbrief Beveiliging nieuwe infrastructuur (C2000)	Kamerbrief Beveiliging nieuwe infrastructuur mobiele communicatie (C2000).pdf	Ministerie van Justitie en Veiligheid	26-4-2019
51.	Bezoekverslag ESN	20190910 Bezoek ESN.docx	Ministerie van JenV	10-9-2019
52.	Bezoekverslag Motorola Expercience centre	20200113 Bezoek Motorola Experience centre.docx	Ministerie van JenV	13-1-2020
53.	Bezoekverslag Erillisverkot	20190904 Bezoek Erillisverkot.docx	Ministerie van JenV	4-9-2019
54.	Landelijk convenant gegevensverwerking meldkamers	20181001-BRWNL-et-al-Landelijk-convenant-gegevensverwerking-meldkamers.pdf	Instituut Fysieke Veiligheid	1-10-2018
55.	Uitvoeringsregeling Informatiebeveiliging Politie	I150108 - Uitvoeringsregeling Informatiebeveiliging Dienst ICT Politie Intern v2.0 getekend.pdf	Politie (dienst ICT)	8-6-2018

56.	Virve Procurement status	CCBG21-22 Virve 2_Phase1-core-and-Ran-service_Kari-Junttila.pdf	Erillisverkot	23-4-2020
57.	Main Findings on RFI Mission critical services	CCBG21-23 Virve2_Phase2-MCx-services-RFI-Findings_Ari-Toivonen.pdf	Erillisverkot	22-4-2020
58.	AIVD politieke samenvatting 5G	5G Politiek samenvatting.pptx	AIVD	29-5-2020
59.	Algemene bevindingen marktconsultatie MNO's 2018	180917 Algemene bevindingen marktconsultatie Breedband OOV v 1.0 DEF.pdf	Ministerie van JenV	17-9-2018
60.	Overzicht van ESN ontwikkelingen in 2019	About the Emergency Service Network ESMCP2019	VK overheid en persbericht Computer Weekly	4-10-2019
61.	Gemiddeld data gebruik per maand per operator	Tefficient industry analysis 1-2020 mobile data usage and revenue for yr 2019 per operator	Tefficient	14-4-2020
62.	Update on ESN	181008 Philip Rutman update on ESN	Philip Rutman	8-10-2018
63.	Annual report on major projects 2019, ESN	IPA AR MajorProjects 2018-2019 web.pdf	IPA	2019
64.	3GPP MCX update SA WG6	3GPP MCX rel plan 7-suresh-chiturri.pdf	Suresh Chiturri (Samsung)	jun-19
65.	EE selected for ESN	EE selected to deliver critical new 4G voice and data network for Britain's Emergency Services	Olaf Swantee CEO EE	10-12-2015
66.	Mediabericht AT&T FirstNet	AT&T CFO says 5G national coverage by mid 2020	John Stephens CFO AT&T	16-5-2019

A.3 Onderzoekscriteria detailuitwerking

Indeling Criteria en beschrijving per sub criterium

Categorie	Criterium	Toelichting	Weging
1. Strategisch / politiek			100%
	1.1: Mate van zeggenschap om nationale economische, politieke en/of veiligheidsbelangen te kunnen borgen (sturing)	Hiermee wordt bedoeld de mate waarin politieke, langere termijn strategische en functionaliteit overstijgende belangen en doelen (kunnen) worden ondersteund.	40%
	1.2: Mate van onafhankelijkheid van leveranciers	Hiermee wordt gedoeld op de mogelijkheden en het gemak waarmee leveranciers, indien gewenst en/of noodzakelijk, kunnen worden gekozen en/of vervangen (bij verwerving en na afloop van contractstermijn).	10%
	1.3: Passend in internationale politieke samenwerkingen	Hiermee wordt bedoeld de mate waarin geo-politieke belangen en doelen (kunnen) worden ondersteund.	20%
	1.4: Mate van zeggenschap om een zekere (minimale) operationele beschikbaarheid bij calamiteiten/rampen te kunnen borgen.	Mogelijkheden om bijvoorbeeld middels priority calling en andere mechanismen bij crisis- en rampen situaties voldoende capaciteit voor operationeel gebruik beschikbaar te houden.	30%
2. Techniek			100%
	2.1: Functionele Beschikbaarheid	De mate waarin de **functionele beschikbaarheid** die de oplossing kan garanderen de 100% benadert. Met de functionele beschikbaarheid wordt bedoeld dat het systeem daadwerkelijk bruikbaar met volledige functionaliteit is voor alle groepen eindgebruikers voor alle ondersteunde gegevensstromen.	30%

2.2: Technische Beschikbaarheid	De mate waarin de **technische beschikbaarheid** die de oplossing kan garanderen de 100% benadert. Met de technische beschikbaarheid wordt de beschikbaarheid van de infrastructuur bedoeld inclusief de inzet van redundante voorzieningen.	5%
2.3: Buitenhuisdekking	De mate waarin de oplossing voorziet in en de mogelijkheden biedt voor een buitenhuis radiodekking (outdoor) van 100% (dus deze zo veel mogelijk benadert) voor een handheld device. De feitelijke radiodekking buitenshuis hangt af van vele factoren, waaronder het aantal zendmasten, locatie van masten, celgrootte (afhankelijk van beschikbare frequenties) en dergelijke. De operationele dekking conform huidige C2000 is incl. 10 km grens-, 33 km zee- en air-ground-air-dekking t.b.v. helikopters en kustwacht.	5%
2.4: Binnenhuisdekking	De mate waarin de oplossing voorziet in en de mogelijkheden biedt voor een radiodekking (indoor) van 100% (dus deze zo veel mogelijk benadert) op gewone locaties als ook op specifieke locaties (special coverage locations): tunnels, ziekenhuizen, industriële complexen, luchthavens, gevangenissen et cetera.	5%
2.5: Capaciteit	Aspecten die hierbij van belang zijn: - Mate waarin het systeem in staat is om reguliere piekbelasting aan te kunnen (dagelijks operationeel gebruik). - Mate waarin het systeem in staat is om zowel gepland als direct (< 5 minuten) capaciteit te kunnen opschalen bij evenementen en calamiteiten.	5%
2.6: Fallback	De mate waarin de oplossing in te bedenken situaties voorziet in fallback of mogelijkheden daartoe aldan niet met beperkte functionaleit en/of capaciteit. Hieronder valt ook de mogelijkheid van pre-emptive toegang, het gebruik van Proximity services en off-net gebruik.	5%
2.7: Functionaliteit	Algemeen functionaliteit: het betreft de functionaliteit die onderdeel uit maakt van het mobiele breedband netwerk	5%

	Spraakdiensten: de mate waarin de oplossing voorziet in de functionaliteit voor **spraakdiensten** die aansluiten bij de werkprocessen (zoals push to talk, direct mode (DMO), groepsgesprekken, koppelen groepen, interconnectie, prioriteit, passive scanning, noodknop, meldkamerfuncties en dergelijke).	5%
	Datadiensten: de mate waarin de oplossing voorziet in de functionaliteit voor **datadiensten**: zoals messaging, generieke IP connectiviteit t.b.v. mobile apps, videostreaming (bodycams, vaste en mobiele cams, drones en dergelijke).	5%
	Specifieke functionaliteit: de mate waarin de oplossing voorziet in **gedifferentieerde functies voor specifieke doelgroepen**. De functionaliteit van de oplossing bestaat uit basisfunctionaliteit van spraak- en datadiensten voor alle gebruikers en voorziet in gedifferentieerde functies voor specifieke doelgroepen, zoals meeluisteren (MIVD/AIVD) (andere voorbeelden vanuit OOV-organisaties nog aan te reiken).	5%
	Gebruiksgemak: de mate van eenvoud en intuïtief gebruik van de oplossing, zowel in de operatie als het beheer, door eindgebruikers/hulpverleners, zowel van dienst als randapparatuur.	5%
2.8: Open standaarden	De mate waarin de oplossing is gebaseerd op open standaarden, nu en in de nabije toekomst om diensten en (rand)apparatuur te kunnen gebruiken van verschillende leveranciers. De mate waarin dit plaatsvindt binnen een ecosysteem dat voor de OOV-organisaties toekomstvast is (minimaal 10 jaar na introductie). Standaarden voor interoperabiliteit in hybride scenario (release 15 en 16 3GPP en verder).	5%
2.9: Interoperabiliteit / koppelvlakken	De mate waarin het mogelijk is om koppelingen met aanpalende systemen te realiseren, zoals met het huidige C2000 systeem (migratie), meldkamersysteem, brandmeldsystemen, et cetera.	5%

	2.10: Alarmering (Paging)	De mate waarin en de wijze waarop alarmering (nu via paging) in de oplossing is opgenomen en de mate van integratie daarvan met de overige functionele stromen.	5%
	2.11: Volwassenheid van oplossing (proven technology)	De mate waarin is aangetoond dat de oplossing volwassen is (proven technology) door voorbeelden van succesvolle implementaties en/of pilots in andere landen en/of sectoren.	5%
3. Beveiliging			100%
	3.1: Beveiliging van het gehele systeem	De mate waarin beveiliging in de oplossing kan voldoen op basis van de huidige geldende standaarden, wet- en regelgeving. Belangrijk om hierbij voor ogen te houden zijn: - Opzet (Is het beschreven?), - Bestaan (Is het daadwerkelijk ingericht?) en - Werking (Functioneert het aantoonbaar?). Zowel logische als fysieke beveiliging (zoals bij de opstelpunten) horen hiertoe als ook de mogelijkheid om op afstand randapparatuur (tijdelijk) te uit te sluiten.	40%
	3.2: Exclusiviteit – access control, authenticatie	Zowel randapparatuur, connectiviteit, netwerkvoorzieningen, centrale bediening, beheersystemen. Scheiding van netwerken (o.a. slicing).	10%
	3.3: Vertrouwelijkheid – vercijfering	Mogelijkheden (functionaliteit en techniek) en kwaliteit van vercijfering.	20%
	3.4: Integriteit – weerbaarheid tegen manipulatie	De mogelijkheden om de integriteit van alle (systeem-)gegevens inclusief de communicatie te borgen.	10%
	3.5: Monitoring/logging	De mogelijkheden voor en de mate en kwaliteit van registratie van activiteiten en handelingen (audit trail) zowel operationeel als beheermatig.	20%
			100%

4. Innovatie en toekomstvastheid	4.1: De mate waarin de oplossing wordt doorontwikkeld als ook de levensduur van de oplossing.	De mate en mogelijkheden waarin de oplossing kan doorontwikkelen en ondersteuning kan bieden van toekomstige releases voor 5G (en 6G, dwz het volgen van het releasebeleid van 3GPP) en voor verbeterde MC-functies.	60%
	4.2: De mate waarin de oplossing de doorontwikkeling van diensten en aanvullende functionaliteit faciliteert en/of ondersteunt.	De mate en mogelijkheden waarin de oplossing nieuwe use-cases kan ondersteunen t.b.v. communicatie zoals bijv. m2m, sensor data, alertering, situational video awareness combined sources.	40%
5. Frequentie spectrum			100%
	5.1: Spectrum efficiëntie	De mate waarin het voor de OOV-organisaties benodigde frequentiespectrum efficiënt gebruikt wordt (dedicated vs shared use) als ook de mogelijkheden van spectrum sharing.	25%
	5.2: Capaciteit	De mate waarin het benodigde frequentiespectrum beschikbaar is voor de noodzakelijke capaciteit (zowel regulier gebruik als bij evenementen en calamiteiten) dan wel door de overheid beschikbaar gemaakt kan worden.	75%
6. Organisatie			100%
	6.1: Projectorganisatie (verwerving systeem)	Mate van inspanning en complexiteit van de organisatie die aan de kant van de opdrachtgever nodig is (zowel kwantitatief als kwalitatief) om de dienstverlening te verwerven en in te richten.	50%
	6.2: Benodigde (beheer)organisatie (exploitatie)	Mate van inspanning en complexiteit van de organisatie die aan de kant van de opdrachtgever nodig is (zowel kwantitatief als kwalitatief) om de dienstverlening in stand te houden.	50%
7. Financieel			0%

	7.1: Business case	Afweging van de (soorten) kosten en mogelijke baten met een verbijzondering naar Projectkosten, Initiële investeringen, transitiekosten, kosten voor frequentie (verwerving en gebruik) en Operationele kosten als ookverschillen in Opex/Capex.	0%
8. Besturing	Bestuurlijke inrichting en de rolverdeling tussen opdrachtgever en opdrachtnemer. Voor- en nadelen per oplossing t.a.v. de bestuurlijke inrichting, inclusief de afweging om (onderdelen) zelf te doen dan wel uit te besteden.		100%
	8.1: Functionele en technische inrichting	De mate van invloed van opdrachtgever op keuzes in de **functionele en technische inrichting** van de oplossing (technische interfaces en koppelvlakken) en de stabiliteit (updates/upgrades).	40%
	8.2: Operationeel beheer	De mate van invloed van opdrachtgever op inrichting operationeel beheer: zelf doen of uitbesteden? Hieronder valt ook de (transparantie) van prestaties van oplossing / dienst (conform OLA/SLA). Wil/kan de opdrachtgever actief meekijken en in kunnen grijpen of is een rapportage voldoende?	40%
	8.3: Toekomstige verbeteringen	De mate van invloed van opdrachtgever op invoering van **toekomstige verbeteringen**, nieuwe functionaliteit, andere gebruikersgroepen en het bestaan van een long term roadmap.	20%
9. Juridisch	De mate waarin juridische aspecten van toepassing zijn op de oplossing en welke. Juridisch mogelijk relevante onderdelen zijn:		100%
	9.1: Beschikbaarheid spectrum / veiling	Waaronder de mogelijkheden van spectrum sharing met andere partijen.	10%
	9.2: Privacy-aspecten		10%
	9.3: Bewijsgaring, bewijsvoering		10%
	9.4: Mededingingswetgeving		30%

	9.5: Aanbestedingswetgeving	10%
	9.6: Telecomwetgeving (incl. netneutraliteit)	30%
10. Tijd / planning	De mate waarin verwacht mag worden dat de oplossing in 2025 beschikbaar is en van 2025-2035 gebruikt kan worden. Bij dit criterium komt een aantal aspecten naar voren:	100%
	10.1: Releaseplanning 3GPP, en de tijd om het systeem te ontwikkelen, testen en operationeel te maken	10%
	10.2: Tijd voor verwerving/aanbesteding (4 – 6 jaar)	30%
	10.3: Tijdpaden wanneer een oplossing beschikbaar is	30%
	10.4: Afhankelijkheden van andere ontwikkelingen: (Veiling 5G, GSM-R en ERTMS, Schiphol aanbesteding, smart meter, et cetera).	10%
	10.5: Ontwikkeling van 4G LTE naar 5G en mogelijke opvolgers.	10%
	10.6: Hoe lang kan nog worden gewerkt met 4G, TETRA, FLEX ™ et cetera?	10%
11. Internationaal		100%

	11.1: De mate waarin internationale ontwikkelingen kunnen bijdragen aan en/of worden opgenomen in de oplossing.	EU-ontwikkelingen zoals EU Broadway voor een compleet next-generation PPDR-systeem (nu in pre-commercial procurement). De eventuele voordelen van een universeel handheld wereldwijd. Het Eco-systeem en de voor- en nadelen daarvan.	40%
	11.2: 3GPP standaarden		20%
	11.3: Mate van mogelijke operationele afstemming met de omringende landen	Hiermee worden de mogelijkheden bedoeld die de oplossing biedt voor directe operationele samenwerking en afstemming met de directe buurlanden, de EU-landen en aan de EU gelieerde landen.	20%
	11.4: Grensoverschrijdende dekking (roaming)	De mate waarin de oplossing voorziet in en de mogelijkheden biedt voor dekking in de grensgebieden, in de buurlanden, in de EU en in de rest van de wereld.	20%
12. Migratie	Mate waarin vanuit de huidige situatie de gewenste doelsituatie zonder onderbreking en met minimale belasting van de eindgebruikers kan worden bereikt. Aspecten die hierbij een rol spelen zijn:		100%
	12.1: Mogelijkheid om onafhankelijk van de huidige oplossing te migreren		20%
	12.2: Eenvoud van migratie.		40%
	12.3: Storingsvrije migratie.	Waaronder ook de mate van interoperabiliteit met huidige netwerk.	40%
13. Risico’s	Criterium overstijgende kansen/risico's zijn opgenomen binnen de categorie Risico's. Voor zover kansen en risico's direct bij een criterium horen, worden die bij dat betreffende criterium opgenomen.		100%
	13.1: Risico’s van de oplossing (functioneel/techniek, tijdslijnen, kosten, organisatie, juridisch).	De mate waarin de oplossing risico’s kent, de eventuele effecten van de betreffende risico’s en de mate van gevoeligheid voor die risico’s (kwantitatieve en kwalitatieve afweging).	75%

13.2: Kansen vanuit de oplossing die kunnen bijdragen aan verbeteringen.	De mate waarin de oplossing kansen kent, de eventuele effecten van de kansen en de slagingskans om een kans te kunnen verzilveren (kwantitatieve en kwalitatieve afweging).	25%

A.4 Uitwerking frequentiespectrum behoefte

In deze bijlage is de frequentiespectrum behoefte van OOV in detail uitgewerkt.

Zowel voor een eigen missiekritisch mobiel breedbandnetwerk als ook voor het gebruik van het netwerk van een mobiele operator is er behoefte aan frequentiespectrum. TNO heeft in 2017 onderzoek gedaan naar onder andere de spectrumbehoefte voor OOV-organisaties[19]. Hierbij heeft TNO een aantal gebruiksscenario's uitgewerkt die wij als uitgangspunt hebben genomen om de behoefte aan frequentiespectrum te kunnen inschatten. Bij missiekritische toepassingen is er een aanzienlijk verschil tussen de behoefte in een normale operationele situatie en die in het geval van calamiteiten. De eigenschap van calamiteiten is dat vooraf niet te voorspellen is waar een calamiteit zich zal voordoen en wat de consequentie is voor de belasting van het netwerk. Bij het ontwerpen van een mobiel netwerk moet er dus van uitgegaan worden dat een calamiteit zich overal kan voordoen en dat dan de benodigde capaciteit voorhanden is. De meest kritische locatie voor een mobiel netwerk is aan de rand van een netwerkcel; daar is de beschikbare capaciteit slechts ongeveer 10% van de capaciteit direct naast het antenne-opstelpunt. Daarnaast zal ook voor de normale, niet-calamiteit situatie een gegarandeerde minimale capaciteit aan de rand van een netwerkcel beschikbaar moeten zijn.

Voor de behoefte aan spectrum zijn er drie scenario's door TNO uitgewerkt[20]: 1. Stedelijke omgeving; 2. Een overstromingsramp; 3. Een verkeersongeval.

De behoefte aan bandbreedte per scenario is:

- Stedelijk scenario: UL (Uplink) 2.6Mbps, DL (Downlink) 2.1Mbps per cel
- Overstroming scenario: UL 6.6Mbps, DL 3.1Mbs per cel
- Verkeersongeval scenario: UL 6,6Mbps, DL 3,1Mbs per cel
- Spraak: UL 0,5Mbps, DL 0,5Mbps per cel

Het maximum van de drie scenario's is een Uplink snelheid van 6,6+0,5=7,1Mbps en een Downlink snelheid van 3,1Mbps + 0,5Mbps = 3,6Mbps. Omdat deze snelheid binnen het gehele netwerk gegarandeerd moet worden dient de benodigde snelheid ook aan de celranden beschikbaar te zijn. Dit houdt in dat de capaciteit waarmee rekening gehouden moet worden een factor 10 hoger ligt, dus 71Mbps Uplink en 36Mbps Downlink.

Met 20MHz bandbreedte is de maximale Uplink 51Mbps. Om een Uplink snelheid van 71Mbps te kunnen realiseren is een Uplink bandbreedte noodzakelijk van 30MHz (op basis van de onderstaande tabel en uitgangspunt UL Category 4).

[19] Rapport TNO Facilitering missie-kritisch mobiel breedband voor het OOV-domein; brondocument 36

[20] Zie voor de uitwerking het TNO rapport 2017 R11193 paragraaf 3.4; brondocument 36

Table 1. Cell peak throughputs for different bandwidths.

	1.4MHz	3MHz	5MHz	10MHz	15MHz	20MHz
DL (SISO)	4.392 Mbps	11.064 Mbps	18.336 Mbps	36.696 Mbps	55.056 Mbps	75.376 Mbps
DL (MIMO 2×2)	8.784 Mbps	22.128 Mbps	36.672 Mbps	73.392 Mbps	110.112 Mbps	150.752 Mbps
DL (MIMO 4×4)	17.52 Mbps	44.304 Mbps	73.392 Mbps	150.752 Mbps	220.272 Mbps	299.552 Mbps
UL (SIMO MCS=23) Category 4 (16QAM)	2.984 Mbps	7.48 Mbps	12.576 Mbps	25.456 Mbps	37.888 Mbps	51.024 Mbps
UL (SIMO) Category 5 (64QAM)	4.392 Mbps	11.064 Mbps	18.336 Mbps	36.696 Mbps	55.056 Mbps	75.376 Mbps

Figuur 30. Bandbreedte vs frequentiespectrum tabel

Voor een zogenoemd FDD (Frequency Division Duplex) mobiel breedband netwerk is dan 2x 30MHz spectrum vereist (30MHz voor de Uplink en 30MHz voor de Downlink). Omdat in een zogenoemd TDD (Time Division Duplex) netwerk de spectrum omvang voor de UL en DL niet identiek hoeft te zijn zou voor een TDD-oplossing volstaan kunnen worden met 1x 45MHz.

Indien voor de landelijke verkeerscapaciteit rekening gehouden wordt met het stedelijke scenario als basis scenario dan is de spectrum behoefte voor FDD 2x 15MHz of voor TDD 1x25 MHz voor 2,6+0,5=3,1Mbps Uplink en 2,1+0,5=2,6Mbps Downlink.

Wil het netwerk voorbereid zijn op een dergelijke verkeerscapaciteit waar dan ook in Nederland dan moet het genoemde spectrum wel in heel Nederland beschikbaar zijn.

In Nederland is per 1 januari 2020 2x 3MHz en 2x 5MHz aangewezen voor Justitie en Veiligheid in de 700MHz-band. Met dit spectrum kan circa 2Mbps Uplink snelheid gerealiseerd worden aan de celranden van het netwerk. Dit beschikbare spectrum is dus zeker niet toereikend om de scenario's die TNO uitgewerkt heeft te kunnen ondersteunen. Opgemerkt moet worden dat de 2x 5MHz op dit moment niet inzetbaar is ten gevolge van het ontbreken van een ecosysteem van beschikbare apparatuur in deze frequentieband.

A.5 Externe bijlagen

- Bijlage 1 Haalbaarheidsonderzoek missiekritische communicatie - Kwalitatieve criteria beoordeling v1.0.xlsx
- Bijlage 2 Haalbaarheidsonderzoek missiekritische communicatie – Financiële vergelijking scenario's v1.0.xlsx