

TNO 2025 R12543 – december 2025

Monitor Draadloze Technologie Najaar 2025



Auteurs	Ing. O.P.W. Abbenhuis; S. Agarwal, MSc; Ir. P.M.A.M. Heijnen; Dr. L. Jorguseski; Ir. R. Overduin; Dr. H. Zhang; Ir. M.M.A. Versluis; Dr. Ir. A.P.M. Zwamborn
Rubricering verslag	TNO Public
Titel	TNO Public
Verslagtekst	TNO Public
Aantal pagina's	39
Aantal bijlagen	0
Opdrachtgever	Ministerie van Economische Zaken
Projectnaam	Monitor Draadloze Technologie 2025
Projectnummer	060.63570

Alle rechten voorbehouden

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van TNO.

© 2025 TNO

Inhoudsopgave

Inhoudsopgave	3
1 Inleiding.....	5
1.1 De Monitor Draadloze Technologie.....	5
1.2 Het 'draadloos speelveld'.....	5
2 Medische wearables voor de digitale zorg.....	7
2.1 Inleiding.....	7
2.2 Belang van medische wearables in de digitale zorg	7
2.3 De technologie van de medische wearable	8
2.3.1 Telecommunicatietechnologie.....	8
2.3.2 Sensor- en processingtechnologie.....	9
2.3.3 Uitdagingen.....	10
2.3.4 Voorbeelden van recente medische wearables	11
2.4 Conclusies.....	13
3 Omgaan met de dronedreiging.....	14
3.1 Wat zijn drones?.....	14
3.2 Wat zijn de soorten bedreigingen door drones?.....	15
3.3 Wat zijn algemene beschermingsmaatregelen?.....	15
3.3.1 Breedbandig storen.....	16
3.3.2 Selectief storen.....	16
3.3.3 Geavanceerd/'slim' storen.....	16
3.3.4 Misleiden.....	16
3.3.5 High Power Microwave.....	17
3.3.6 High Energy Laser.....	17
3.4 Voorbeelden van incidenten	18
3.4.1 Nationaal	18
3.4.2 Duitsland.....	19
3.4.3 Polen.....	19
3.4.4 Denemarken	20
3.4.5 Noorwegen.....	20
3.4.6 België.....	20
3.5 Wat gebeurt er bij nationale inzet van tegenmaatregelen?.....	20
3.5.1 Voorbereiding van de mogelijke inzet van tegenmaatregelen tegen drones	20
3.5.2 Overgaan tot inzet: wat mag volgens de AMvB?.....	21
4 5G-implementatie: de huidige stand van zaken	22
4.1 Inleiding.....	22
4.2 5G in Nederland	22
4.2.1 De 3,5 GHz-band in gebruik.....	22
4.2.2 Dekking en snelheid.....	22
4.2.3 5G-gebruikersapparaten en -netwerkelementen	25
4.3 5G in de rest van de wereld.....	25
4.3.1 Milde uitrol van SA 5G met China als koploper	25
4.3.2 5G mobiele gebruikersapparaten en netwerkelementen	26
5 Open RAN: voortgang en perspectieven	28
5.1 Introductie	28
5.2 Belangrijke ontwikkelingen sinds 2021: marktacceptatie en -implementatie.....	28
5.2.1 Ontwikkeling van O-RAN-ondersteuning	28
5.2.2 Ontwikkeling van de O-RAN markt.....	30

5.3	Voortgang in standaardisatie.....	31
5.4	Uitdagingen en <i>lessons learned</i>	32
5.4.1	Greenfield of brownfield-implementaties?.....	32
5.5	Voortgang rond beleid en regelgeving	33
5.6	Conclusies.....	33
6	Update van standaardisatie binnen 3GPP	34
6.1	Inleiding.....	34
6.2	Samenvatting van 6G RAN studies in Release 20	35
6.2.1	Studie naar 6G scenario's/use cases en (RAN) requirements.....	35
6.2.2	Studie naar 6G Radio	35
6.3	Samenvatting van 5G-Advanced RAN-functies en -activiteiten in Release 20	36
7	Tot besluit.....	39

1 Inleiding

Om overzicht te bieden in het speelveld van de diverse draadloze technologieën, stelt TNO sinds een decade een Monitor Draadloze Technologie samen. Hierin worden ontwikkelingen in de technologie en de markt gevolgd.

In dit inleidende hoofdstuk worden de scope en de opzet van de Monitor Draadloze Technologie toegelicht.

1.1 De Monitor Draadloze Technologie

Met de Monitor Draadloze Technologie (kortweg 'de Monitor') wil TNO een degelijk, actueel en toegankelijk overzicht bieden van de stand van zaken ten aanzien van de ontwikkeling en inzet van draadloze technologie. De Monitor Draadloze Technologie wil diverse doelgroepen bedienen bij overheid en bedrijfsleven in Nederland. Dit impliceert dat de Monitor erop gericht is om informatief te zijn voor lezers met een algemene achtergrond in telecommunicatie. Daarbij moet worden aangetekend dat sommige technische onderwerpen specifiek kunnen zijn. Deze onderwerpen vragen naast een algemene beschrijving meestal om meer technische toelichting waardoor ook de meer technisch onderlegde en -geïnteresseerde lezersgroep tegemoet wordt gekomen.

In principe worden wereldwijde ontwikkelingen gevolgd vanuit een nationaal perspectief.

Evenals vorige jaren is gekozen voor de schriftelijke rapportagevorm om de informatie te ontsluiten. Deze bestaat uit twee (halfjaarlijkse) edities, zodat beter kan worden aangesloten op recente trends en ontwikkelingen:

- Een voorjaarseditie met een overzicht van ontwikkelingen vanuit voornamelijk technologisch perspectief. Per technologie wordt kort de stand van zaken beschreven;
- Een najaarseditie die met name gaat over een aantal thema's, trends en toepassingen van draadloze communicatietechnologie. Dit is de editie die u nu leest.

TNO hecht eraan te benadrukken dat de Monitor slechts een momentopname is van een complex en snel veranderend speelveld. Het is daarom mogelijk dat opgenomen informatie op het moment van lezen niet meer up-to-date is, of niet langer relevant. Daarnaast valt niet te ontkomen aan enige willekeur in de keuze van geschetste ontwikkelingen. Het kan dus zijn dat ontwikkelingen die in de ogen van een specifieke lezer zeer relevant zijn, niet worden beschreven. TNO staat open voor suggesties of aanbevelingen voor verdere verbeteringen.

1.2 Het 'draadloos speelveld'

Deze Monitor najaarseditie van 2025 biedt onderwerpen die alle nauw - en soms zeer nauw, aansluiten bij actuele trendbewegingen en gebeurtenissen.

Om te beginnen behandelt Hoofdstuk 2 vanuit diverse invalshoeken medische wearable technologie en wat deze kan betekenen voor patiënten en voor de zorg. Daarbij wordt niet alleen op de draadloze technologie ingegaan, maar juist ook veel op de applicatie en de diverse uitvoeringsvormen.

Hoofdstuk 3 gaat in op de dreiging door drones en vooral hoe hiermee met behulp van draadloze technologie wordt en kan worden omgegaan. Daarbij komen op hoofdlijnen technologische perspectieven aan de orde die in openbare bronnen zijn te vinden. Recente incidenten worden belicht om de realiteit van deze dreiging binnen Nederland en de rest van Europa aan te geven. Tenslotte wordt aangegeven welke mogelijkheden de Nederlandse wetgeving biedt om de dreiging door drones te pareren.

De hoofdstukken 4 tot en met 6 gaan in op technologieontwikkelingen rond mobiele telecommunicatie waarbij de generaties 5G, 5G Advanced en 6G aan de orde komen. In concreto gaat het over achtereenvolgens:

- De stand van zaken rond 5G-implementatie in Nederland en daarbuiten, ingegeven door de beschikbaarstelling van de 3,5 GHz-band in Nederland en de mondiale uitrol van 5G standalone-netwerken;
- De voortgang en perspectieven van Open Radio Access Networks (O-RAN) sinds 2021, waarbij ontwikkelingen rond het ecosysteem, de marktpositie en activiteiten om aan te sluiten bij 3GPP de revue passeren;
- Ook in deze najaarseditie is een update rond de standaardisatie binnen 3GPP opgenomen.

2 Medische wearables voor de digitale zorg

2.1 Inleiding

Medische *wearables* zijn door een patiënt op het lichaam gedragen apparaten zoals *smart patches* of implantaten die gegevens verzamelen over de individuele gezondheid ten behoeve van klinische besluitvorming. Dit is een verschil met veel huidige smartwatches en *fitness trackers* (die specifiek de mate van beweging bijhouden). Deze type devices geven informatie uitsluitend direct, zonder interpretatie door aan de drager. Hierop vormen de smartwatches met een volledige 4G- of 5G-telefoonfunctie de uitzondering. Doorgaans is in het geval van medische wearables bovendien sprake van een nauwkeuriger en meer gedetailleerde, vaak continue gegevensstroom naar digitale gezondheidstools van zorgverleners (in plaats van uitsluitend naar een app van de eigenaar van de smartwatch of fitness tracker). Belangrijke medische grootheden die worden gemeten zijn bloeddruk, hartfunctie, ademhaling, lichaamstemperatuur en het zuurstofgehalte.

Het verzamelen van gegevens van de patiënt naar een hulpverlener kan gezien worden als een belangrijk aspect van de digitale wearable maar het is zeker ook mogelijk dat de informatiestroom van de hulpverlener naar de wearable gericht kan zijn. Deze *flow* bestaat uit sturingscommando's om het apparaat te activeren, bijvoorbeeld voor het starten of stoppen van het verzamelen van gegevens of voor het initiëren van een bepaalde actuator van de wearable zoals het inbrengen van insuline.

2.2 Belang van medische wearables in de digitale zorg

Er zijn diverse redenen waarom medische wearables van groot sociaal-maatschappelijk en economisch belang zijn.

Door de toepassing van wearables wordt het mogelijk om de ziektelast te verlagen en zorg voor patiënten efficiënter en effectiever te maken. De patiënt kan doorlopend, zonder (periodiek) ziekenhuisbezoek worden geobserveerd en heeft deze gegevens zelf ook ter beschikking. Vanuit de patiënt worden, waar deze zich ook bevindt, de medische gegevens verzameld of een lichaamsfunctie geactiveerd met essentieel minder stressvolle ziekenhuisbezoeken waardoor zowel de patiënt als de zorg minder worden belast¹. In het laatste geval impliceert dit tevens kostenreductie. De zorgverlener is in staat om door de langere observatieperiode een nauwkeurigere diagnose te stellen. Bovendien kunnen in kortere tijd veel meer patiënten geanalyseerd worden waarbij sneller patronen herkend en behandelingen aangepast kunnen worden. Een consequentie kan zijn dat kwetsbare groepen zoals ouderen langer veilig thuis kunnen blijven wonen met evidente voordelige implicaties voor de patiënt en zorg zoals eerder benoemd. Tenslotte mag worden gesteld

¹ <https://www.tno.nl/nl/newsroom/insights/2024/06/medische-wearables-betaalbare-zorg/>

dat op termijn wearables de toegang tot de gezondheidszorg van patiënten algemeen maken, dat wil zeggen ongeacht afstand en kosten.

In het bijzonder kunnen in preventief opzicht, door het meten van gezondheidsindicatoren via wearables, gepersonaliseerde gezondheidsadviezen worden gegeven die bijvoorbeeld de leefstijl aangaan en die dus door de patiënt zelf kan worden beïnvloed. Deze continue, directe gegevensbeschikbaarheid (*the quantified self*) verhoogt de individuele bewustwording van wat leefstijl ‘aantoonbaar’ kan betekenen, bijvoorbeeld wat- en in welke mate de slaap beïnvloedt, stress veroorzaakt of hoe gewoonten het glucoseniveau beïnvloeden. Dit motiveert de betrokkene om preventieve gezondheidsmaatregelen te nemen² en uiteindelijk een gedragsverandering in te zetten.

Duidelijk mag zijn dat de grootste voordelen voor betrokkenen en de zorg worden bereikt door consequente en grootschalige preventie.

Het gebruik van medische wearables maakt een belangrijk deel uit van de implementatie van eHealth. Deze implementatie raakt meerdere disciplines en daardoor juridische, ethische, financiële en technologische aspecten en afwegingen³. De overgang van standalone eHealth tools naar geïntegreerde digitale zorgomgevingen waarbij wearables essentiële *enablers* vormen, vereist dan ook de actieve betrokkenheid van partijen binnen al deze disciplines. In het vervolg van dit hoofdstuk zal de nadruk liggen op de technologische aspecten.

2.3 De technologie van de medische wearable

In deze paragraaf wordt achtereenvolgens ingegaan op de telecommunicatietechnologie (2.3.1) en op de sensor- en verwerkingstechnologie van de medische wearable (2.3.2). Vervolgens wordt kort en kwalitatief ingegaan op de technische uitdagingen (2.3.3) en wordt als beeldvorming tenslotte een aantal voorbeelden van recente medische wearables gegeven (2.3.4).

2.3.1 Telecommunicatietechnologie

Algemeen maken medische wearables voor de telecommunicatie met een medische locatie zoals van een huisarts, gezondheidscentrum en dergelijke, gebruik van commerciële, openbare draadloze mobiele technologie. Deze systemen verbeteren met elke generatie op gebied van betrouwbaarheid, veiligheid/privacy en performance, waar snelheid voor medische wearables zeer belangrijk is. De applicaties van wearables, inclusief de medische, zijn dan ook in wezen IoT-toepassingen over deze communicatietechnologieën. Daarnaast kan, afhankelijk van de medische toepassing en de sensor, draadloze communicatie met de mobiele telefoon van de drager op PAN (Personal Area Network)-niveau plaatsvinden via Bluetooth of NFC (Near Field Communications) of op LAN (Local Area Network)-niveau met internet via Wi-Fi. Implantaten kunnen ook van deze technologieën gebruik maken, behalve voor het communiceren tussen implantaten onderling. Hiervoor gelden aparte eisen en wordt gebruik gemaakt van *proprietary* technologie⁴.

Soms wordt, meestal vanuit de Verenigde Staten, een pleidooi gehouden om de medische wearable-communicatie met de medische locatie te laten verlopen via Short Message Service (SMS)⁵. Argumenten die hiervoor worden aangedragen, zijn dat de technische

² <https://3bplus.nl/wearables/>

³ <https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2024.1332707/full>

⁴ <https://mtintegraal.nl/medische-mijlpaal-binnen-de-draadloze-pacemakers-interview-met-cardioloog-louise-olde-nordkamp/>

⁵ <https://www.paubox.com/blog/why-texting-is-the-best-communication-method-for-wearable-technology>

eenvoud achter SMS als bewezen technologie goed kan worden geïmplementeerd op apparaten zoals wearables met beperkte rekenkracht, opslagcapaciteit en accucapaciteit. Verder zou snel, goed beveiligd en energiezuinig het grote totale dataverkeersaanbod dat door wearables wordt gegenereerd, kunnen worden afgehandeld. De energievriendelijke datacommunicatie is een valide argument, maar de andere motieven zijn op de Nederlandse situatie niet of veel minder van toepassing. De conventionele SMS-technologie wordt in Nederland nog wel ondersteund⁶ maar vooral de afleversnelheid kan zeer variabel zijn. Dit is niet toepasbaar in tijd-kritische situaties waarin bijvoorbeeld een gezondheidscentrum of arts de patiënt vrijwel instantaan en veilig moet kunnen bereiken. Eerder ligt voor onder meer Nederland een opvolger van SMS voor de hand, zoals RCS (Rich Communication Services/ Rich Communication Suite)⁷ die inherent goede beveiliging, betrouwbaarheid en privacy-ondersteuning biedt en is toegesneden op de pakket-geschakelde infrastructuur waarop mobiele netwerken sinds 4G zijn gebaseerd. Bovendien voorziet GSMA (GSM Association) in een gedegen standaardisatie van RCS in Europa waardoor ondersteuning door MNO's (Mobile Network Operators) ook op langere termijn waarschijnlijk wordt.

Hoe dan ook zal de zesde generatie mobiele technologie wellicht meer perspectief bieden, waar 6G onder meer door toepassing van *slicing*-technologie en energiebeperkende maatregelen aan de bezwaren van privacy-gevoeligheid en energieconsumptie van medische wearables tegemoet kan komen. Ook zal AI (Artificial Intelligence) in 6G-apparatuur geïntegreerd zijn (*native AI*) waardoor de samenwerking met bestaande processen en -data directer en dus eenvoudiger en efficiënter kan. Verder zal de ambitie om de performance van 6G in vergelijking tot die van 5G een orde-grootte te verbeteren, leiden tot meer perspectief voor tijdige en betrouwbare verwerking van (nog) meer gelijktijdige datastromen, in dit geval van en naar medische wearables. Bij een grootschalige gebruiksdichtheid zoals verwacht in 6G zal er niettemin voor gezorgd moeten worden dat de beschikbaarheid van voldoende communicatiecapaciteit voor AI-native medische systemen adequaat wordt geregeld⁸.

2.3.2 Sensor- en processingtechnologie

Uit het voorgaande is gebleken dat geschikte communicatie voor medische wearables neerkomt op snelle, betrouwbare en adequaat beveiligde IoT-technologie. Interessant is het dan ook om inzicht te krijgen in de mogelijkheden van draagbare sensoren (de eigenlijke wearables) en hun verwerkingsmogelijkheden en daarmee de datastromen die nu en in de nabije toekomst ondersteund moeten kunnen worden. Het vervolg van dit hoofdstuk besteedt dan ook ruime aandacht aan de toepassingsmogelijkheden van dit type gebruikersterminal, dat wil zeggen de sensor- en verwerkings- c.q. *processing*-functionaliteiten.

2.3.2.1 Processingtechnologie

Voor wat betreft de gegevensverwerking wordt in toenemende mate AI, in de vorm van *wearable AI*, belangrijk. Het 'slim' combineren van diverse individuele medische data over een bepaalde periode kan leiden tot een snelle ondersteuning van analyses en diagnoses, idealiter zelfs tot ondersteuning in preventieve zin⁹. Zo kan de wearable op basis van verzamelde trends autonoom signalen afgeven om bijvoorbeeld water te drinken, dieper te ademen (om stress te verminderen) of de glucosespiegel te controleren (ondersteuning bij

⁶ TNO 2023 R11093, juni 2023, blz. 13

⁷ TNO 2023 R11093, juni 2023, blz. 13-16

⁸ <https://www.sciencedirect.com/science/article/pii/S2352864825001038>

⁹ <https://litslink.com/blog/ai-wearables>

diabetes). Hierdoor is dus sprake van een directe, snelle terugkoppeling naar de drager, zonder tussenkomst van een hulpverlener. In de toekomst zal door deze tendens de aanvankelijke definitie van medische wearable uit Paragraaf 2.1 onder druk komen te staan: de interpretatie en vervolgens de medische adviezen die nu nog door een medisch deskundige worden uitgevoerd, zijn hier dus in principe geautomatiseerd. Zodra gegevens van diverse sensoren zijn verzameld, beginnen wearables met ML (Machine Learning) deze te analyseren en ontdekken patronen terwijl bovendien de verwerking na verloop van tijd verbetert. Zo kan de wearable een piek van de hartslag op elke maandagochtend vaststellen. Koppeling aan het slaappatroon kan een indicatie geven voor stress zodat de wearable een trigger afgeeft voor een ademhalingsoefening. In deze lijn is het zeker denkbaar dat wearable AI-technologie kan functioneren als *early warner* voor bijvoorbeeld een naderend hartinfarct of een beroerte, zelfs nog zonder dat zich symptomen hebben geopenbaard.

Niettemin is het ondanks deze trend waarbij de grens van de medische wearable en een fitness tracker/smartwatch vervaagt, voorstelbaar dat een beoordeling van een medisch deskundige in de nodige situaties van belang blijft, alleen al om niet (altijd) volledig blind te varen op AI-technologie.

2.3.2.2 Sensortechnologie

Wearable sensoren zijn er in vele uitvoeringen. Zo zijn er *smart patches* die op de huid worden geplakt voor het meten van de hydratatie of glucosespiegel zonder dat er bloed hoeft te worden afgenomen. Ook kunnen oordopjes de hartslag en ademhaling registreren. Tenslotte zijn er de meer traditionele pols-wearables en zelfs als sierraden gedragen uitvoeringen zoals hoofdbanden of de *smart ring* waarover later meer.

De bloeddruk is een van de meest belangrijke markers aangezien bloeddrukwaarden (en veranderingen hierin) een hoge indicatieve waarde hebben voor de gezondheid en de mogelijke ontwikkeling hiervan. Juist het meten van deze marker met adequate nauwkeurigheid via acceptabel kleine wearables vormt een specifieke uitdaging.

2.3.3 Uitdagingen

Tabel 1 geeft een beeld van de algemene technische uitdagingen voor medische AI-empowered wearables en hoe de industrie deze aanpakt¹⁰.

¹⁰ <https://litslink.com/blog/ai-wearables, Challenges and considerations>

Tabel 1: Technische uitdagingen voor medische AI-empowered wearables en oplossingsrichtingen
[bron: Litslink, aangepast]

uitdaging	toelichting	huidige oplossingsrichtingen
Data Privacy	Gezondheidsgegevens kunnen worden gehackt of misbruikt.	Gebruik van adequate end-to-end-encryptie, veilige cloudopslag en strikte access control.
Nauwkeurigheid en betrouwbaarheid	Onjuiste metingen kunnen gemiste waarschuwingen of ongegronde angst door <i>false alarms</i> veroorzaken.	Betere sensoren, continue algoritme-updates en klinische validatie.
Kosten en toegankelijkheid	Niet iedereen kan zich het nieuwste apparaat veroorloven.	Verbetering door massaproductie, subsidies en de toepassing van open-source technologie.
Technische vaardigheid	Sommige gebruikers vinden de installatie/configuratie of de tracking te complex.	Eenvoudigere gebruikers-interfaces en begeleiding bij installatie. Meertalige ondersteuning.
Interoperabiliteit van apparatuur	Wearables maken mogelijk geen verbinding met een systeem of app.	Toenemend gebruik van open standaarden. API-integratie in de gezondheidszorg.
Batterijvoeding en duurzaamheid	Apparaten moeten langere tijd betrouwbaar kunnen werken.	Duurzamere ontwerpen en langere batterijduur in nieuwere modellen.

2.3.4 Voorbeelden van recente medische wearables

In deze paragraaf wordt ingegaan op uiteenlopende medische wearables die recent verkrijgbaar zijn of op korte termijn op de markt zullen verschijnen¹¹. Dit productoverzicht is verre van compleet maar wil vooral een indruk geven van de diversiteit aan medische wearables en de achterliggende technologieën. Soms zijn dit geen medische wearables in de oorspronkelijke zin, die een directe communicatielijn met een medische locatie bieden, maar het bevestigt wel de trend dat de grens tussen de traditionele medische wearables en de fitness trackers/smartwatch vervaagt.

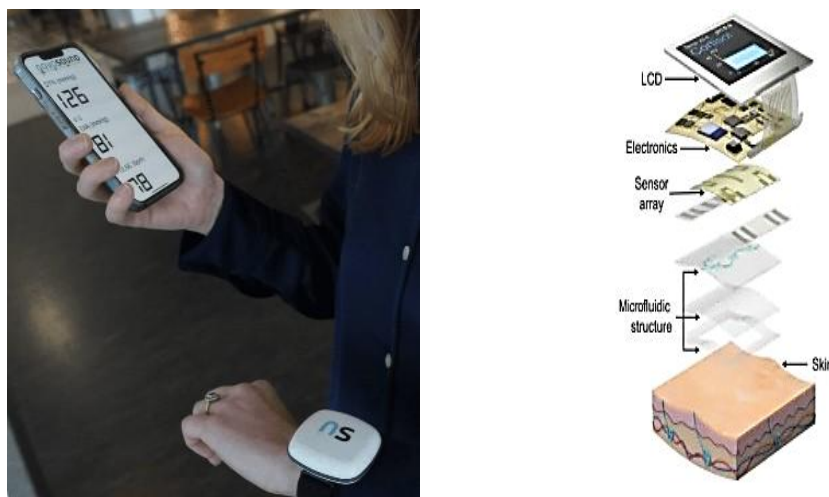
Met de Schotse **Novosound technologie** voor het meten van bloeddruk worden de afmetingen en resonanties van de slagaderwand gemeten om de spanning in de slagaderwand te bepalen, zie Figuur 1, links. Deze staat in direct verband met de bloeddruk waardoor een nauwkeurigheid wordt geclaimd die vergelijkbaar is met traditionele manchetmetingen. Door sensoren en actuatoren in flexibele dunne film-technologie uit te voeren, kunnen zij in een (nog wat grote) wearable worden geïntegreerd en worden ultrasone signalen gegenereerd die door de huid kunnen dringen. Het weerkaatste ultrasone signaal bevat de benodigde informatie. Er wordt dan ook gesproken van echografie. De metingen zijn continue, zonder dat uitwendige mechanische spanning hoeft te worden aangebracht.

Bij de optische methode (photoplethysmography of PPG) wordt licht door de huid gezonden. De verandering in lichtabsorptie is een maat voor de bloeddruk. Een meting duurt 30 seconden. Juist in het laatste jaar is de nauwkeurigheid van draagbare bloeddrukmeters

¹¹ <https://thaumatec.com/knowledge/blog-posts/thaumatec-healthtech-industry-update-new-medtech-wearable-sensors-in-2025/>

aanzienlijk verbeterd door de ultrasound methode, c.q. echografie. Hoewel PPG-meters nauwkeurig kunnen zijn bij correct gebruik en kalibratie met standaardmetingen, zijn ze niet geschikt voor continue monitoring of metingen in bepaalde situaties. Echografie-wearables zijn bovendien handiger, met real-time gegevens direct vanaf de pols.

In Californië is aan de UCLA in 2022 de **CortiSense** ontwikkeld die in staat is via uiterst kleine transpiratievochtdeeltjes doorlopend cortisol niveaus te meten. Een opnamer met daarin gemanipuleerde DNA-strengen (aptameren) detecteert veranderingen als gevolg van cortisol die worden omgezet in een elektrisch signaal, zie Figuur 1, rechts.



Figuur 1: De echografische oplossing van Novosound (l) en de opbouw van de CortiSense sensor (r)

Het doorlopend meten van het cortisol-niveau biedt de drager inzicht in het verloop van zijn of haar stressniveau gedurende de dag waardoor het in principe mogelijk wordt deze zelf te managen. In een uiterst geval kan de aanloop naar een burnout worden waargenomen.

De **Smart Ring** betreft een discreet ontworpen device die als een ring gedragen wordt en continue diverse vitale markers kan meten die worden doorgegeven via Bluetooth aan een app. De indruk bestaat dat de smart ring is ontworpen om de tendens in de gezondheid vast te stellen (*fitness tracking*), waardoor de absolute meetnauwkeurigheid wat minder van belang lijkt. De meeste smart rings volgen slaappatronen, activiteitsniveaus en stress. Het nauwkeurig meten van bloeddruk met een smart ring is nog onderhevig aan onderzoek.

Er zijn diverse smart rings op de markt zoals de Aabo ring, Kuinha Fitness Tracker, Oura Ring Gen 4, Samsung Galaxy Ring, Ultrahuman Ring Air. Prijsverschillen zijn groot en onder meer afhankelijk van materialen en toegepaste sensortechnologieën. Een voordeel van de smart ring is de relatief lange batterijduur waardoor dit device langer achtereen actief kan blijven.

Specifiek voor de gezondheid van vrouwen, richt de **Peri AI-enabled tracker** zich op het volgen van symptomen die verband houden met de perimenopauze. Dit device is dit jaar op de markt gekomen en past AI-algoritmen toe die zijn gebaseerd op driejarig onderzoek en verzamelde data van vrouwen tijdens deze levensperiode. De Peri tracker verzamelt doorlopend huidgegevens zoals transpiratie en temperatuur en wordt op de torso gedragen. Hierdoor zou dit vooral 's nachts tot praktische comfortproblemen kunnen leiden.

Het **FlowBeams BoldJet** draagbare sensor en naaldvrij injectiesysteem is ontworpen om via laser en microfluïde-technologie injecties van diverse aard toe te dienen via de zogenoemde *microjet*. Hierbij worden diverse gegevens bepaald en/of uitgewisseld via BLE (Bluetooth Low Energy) zoals patiënt-specifieke informatie (allergie, huidig medicijngebruik, et cetera), de

dosering, de injectielocatie op de huid en de terugkoppeling van de status van de laser en het microfluïde-systeem en de kwaliteit van de injectie.

Dit device doseert vloeistof microjets die met een snelheid van ruim 300 km/u doordringen tot in de oppervlakkige huidlagen. Een laser wordt gebruikt om de medicatie te verhitten, waardoor een microbel ontstaat die uitzet en de medicatievloeistof voortstuwt. De injectiediepte wordt nauwkeurig gecontroleerd en betreft specifieke huidlagen (opperhuid en lederhuid) voor optimale absorptie. Dit concept biedt de patiënt comfort, draagt bij aan de reductie van medisch afval en de toepassing vergt alleen een basale training.

2.4 Conclusies

Wearable technologie biedt in potentie wezenlijke mogelijkheden en voordelen voor zowel de dragers als voor de gezondheidszorg, zowel in termen van kwaliteit, welzijn en comfort als op het gebied van kostenreductie. De potentie van wearable technologie voor zorgpreventie kan gezien worden als de meest impactvolle, zeker op termijn.

Medische wearables zijn te beschouwen als vorm van ‘hoogwaardige’ IoT-toepassingen met als *key performance indicators* betrouwbaarheid, veiligheid/privacy en snelheid. Daarbij neemt ook de diversiteit aan toepassingen toe.

Er zijn op diverse vlakken nog uitdagingen maar deze hebben al de aandacht van de industrie, internationale standaardisatie en wetgeving.

De datastromen worden gekarakteriseerd door een kleine datavolume per flow maar naar verwachting kunnen er in de toekomst veel gebruikers zijn en dus navenant veel gelijktijdige *flows* die betrouwbaar en beveiligd/ afgeschermd moeten zijn. Veel is wat communicatieondersteuning betreft al mogelijk in de huidige generaties mobiele systemen maar 6G biedt ten opzichte van deze generaties nog meer potentieel.

Tegelijkertijd tenderen de traditionele medische wearables meer naar autonome fitness trackers of smart watches. De rol van AI speelt een grote rol bij de totstandkoming van deze autonomie. Tot op zekere hoogte zouden de interpretatie van meetdata en de daarmee samenhangende medische adviezen technisch geautomatiseerd kunnen worden. Het is daarbij wel de verwachting dat de beoordeling van een medisch deskundige in bepaalde gevallen van belang blijft.

Juist voor de zorgpreventie zijn AI-empowered wearable systemen veelbelovend.

3 Omgaan met de dronedreiging

3.1 Wat zijn drones?

Met een drone wordt over het algemeen een luchtvaartuig zonder piloot aan boord bedoeld ofwel een onbemand luchtvaartuig (definitie volgens de Federal Aviation Administration en tevens conform Verordening (EU) 2018/1139). Het kan daarbij gaan om een luchtvaartuig dat gevlogen wordt door een piloot-op-afstand (de *controller*, hierna kortweg 'piloot') of om een variant die autonoom kan vliegen op basis van een voorgeprogrammeerde vliegroute. Drones zijn vaak uitgevoerd als multi-rotor *devices* (quad- of octo-copters) of als luchtvaartuigen met vaste vleugels (*fixed wing*) zoals de in 2018 door Defensie aangeschafte MQ9 Reapers. Veel commerciële drone-uitvoeringen zijn relatief klein en bovendien meestal publiek te verkrijgen voor zowel professioneel gebruik als anderszins. Binnen de NAVO wordt dan ook vooral gesproken over small Uncrewed/Unmanned Aerial Vehicles (sUAV's).

In dit hoofdstuk beschouwen wij vooral de drone die op afstand bestuurd wordt en duiden we deze in het vervolg aan met drone. Alleen daar waar het duidelijk gaat om de autonome variant wordt deze als UAV of UAS (Unmanned Aerial System) aangemerkt. Als dit niet duidelijk volgt uit de context, gebruiken we 'drone' als algemene aanduiding.

Aangezien de Monitor betrekking heeft op draadloze technologie, worden in dit hoofdstuk drones met glasvezelverbindingen buiten beschouwing gelaten. Primair wordt uitgegaan van *airborne* drones, maar in principe kan de inhoud van dit hoofdstuk ook betrekking hebben op drones die maritiem, boven- of onder water en op het landoppervlak opereren.

De op afstand gevlogen drones zijn voor relatief korte afstanden ontworpen, afhankelijk van de kwaliteit van de draadloze communicatie tot circa 25 km. De autonoom vliegende UAV's kunnen vaak een veel grotere afstand overbruggen, in de orde van 100 km of meer.

Eventuele videobeelden of foto's die dergelijke UAV's opnemen, worden dan meestal via satellietcommunicatie (satcom) of mobiele netwerken overgedragen.

Daarnaast bestaan er drones die gevlogen worden op basis van zicht of door middel van de camerabeelden die op de controller te zien zijn. Deze drones hebben over het algemeen een relatief beperkte maximum snelheid van ongeveer 80 km/u.

Ook bestaan er zogenoemde First-Person-View (FPV) drones¹². Dit zijn drones die zijn ontstaan vanuit de zelfbouwhoek en vanuit de community die met drones racet. Hierbij draagt de controller een soort *virtuality reality*-bril waarop de navigatiebeelden van de drone te zien zijn en krijgt de controller de ervaring alsof hij zich als piloot in de drone bevindt. Dit zijn over het algemeen zeer snelle drones waarbij maximum snelheden tot ver boven de 100 km/u gehaald kunnen worden.

De beperking voor frequentiebeslag door legale drones wordt gevormd door de frequentiebanden die per ITU-regio gebruikt mogen worden. Voor illegale activiteiten houdt men zich hier uiteraard niet aan. Met de gangbare EPM (Electronic Protective Measures)-

¹² <https://droneland.nl/drones/dji/dji-fpv>

technieken aan boord van drones zijn de mogelijkheden daarmee onoverzienbaar en zullen deze drones buiten de “vergunningsvrij zonder meldingsplicht” gealloceerde frequentiebanden goed kunnen opereren.

3.2 Wat zijn de soorten bedreigingen door drones?

Vanwege de verscheidenheid aan publiek verkrijgbare drones en de beschikbaarheid daarvan, zijn deze zeer aantrekkelijk om in te zetten voor illegale activiteiten. Denk hierbij aan het naar binnen smokkelen van verboden spullen boven een penitentiaire inrichting, aan het droppen van bijvoorbeeld een explosief of voor spionage door bijvoorbeeld statelijke actoren.

Daarnaast is deze dreiging continue in ontwikkeling want fabrikanten van drones verbeteren continue de draadloze communicatie in hun producten. Zij doen dit enerzijds om hun product steeds beter te kunnen laten omgaan met toenemende (onderlinge) interferentie zodat de kwaliteit van de radiolink nog voldoende blijft en anderzijds om hun product steeds verder te kunnen laten vliegen. Veel gebruikte termen hierbij zijn: Line-of-Sight (LoS), Beyond-Line-of-Sight (BLoS) en Beyond-Visual-Line-of-Sight (BVLoS). De ervaring leert dat de wat kleinere commerciële drones tijdens het vliegen al snel niet meer zichtbaar zijn met het blote oog.

De draadloze communicatie in drones wordt enerzijds steeds breedbandiger maar anderzijds ook steeds meer adaptief qua gebruik van de spectrumruimte. De chips met draadloze technologie hebben als *enablers* hiervoor een enorm snelle ontwikkeling doorgemaakt, niet alleen door de opmars van drones maar ook vanwege de opkomst van het Internet-of-Things (IoT). Deze chips bieden een steeds groter frequentiebereik waardoor een navenant grotere afzetmarkt wordt bereikt. Hier is een verschuiving te zien van het gebruik van de ISM (Industrial, Scientific and Medical)-banden in de lagere frequenties naar de wereldwijde ISM-band op 2,4 GHz.

3.3 Wat zijn algemene beschermingsmaatregelen?

Tegen de dreiging van drones bestaan diverse soorten bescherming. Veel van deze maatregelen zijn bekend gesteld in openbare bronnen. De inhoud van deze paragraaf (en heel Hoofdstuk 3) is dan ook op publieke bronnen gebaseerd.

Ten eerste kan onderscheid gemaakt worden tussen *soft-kill* en *hard-kill*-maatregelen.

Hard-kill betreft het fysiek aanvallen van drones waarbij vooralsnog gedacht kan worden aan het afvuren van een net op een drone¹³, de drone uit de lucht schieten of met een andere interceptor de drone aanvallen¹⁴.

Soft-kill-maatregelen^{15,16} grijpen de drone niet fysiek aan. Hieronder vallen bijvoorbeeld breedbandig storen (*jammen*), selectief storen, geavanceerd ('slim'/*smart*) storen, misleiden

¹³ <https://www.bnr.nl/nieuws/nieuws-politiek/10587311/defensie-wil-shotguns-en-netgeweren-tegen-drones>

¹⁴ <https://www.defensie.nl/actueel/nieuws/2025/11/25/defensie-investeert-extra-in-middelen-tegen-drones>

¹⁵ <https://acasom.com/blogs/news/how-many-types-of-drone-signal-jammers-do-we-have#:~:text=Wideband%20jammers%20disrupt%20entire%20frequency,tool%20for%20high%20risk%20scenarios.>

¹⁶ <https://xray.greyb.com/drones/anti-jamming-system>

en belichting met High-Power Microwave (HPM) pulsen. Hierbij moet aangetekend worden dat HPM raakt aan hard-kill omdat dit in sommige gevallen kan leiden tot fysieke beschadiging van een drone. Dit kan ook de opzet zijn van het gebruik van High Energy Lasers (HEL). HEL kan ook ingezet worden om optische drone-sensoren te verblinden of te verwarren.

Soft-kill-activiteiten maken gebruik van het elektromagnetisch spectrum en zullen in de volgende paragrafen kort nader worden toegelicht.

3.3.1 Breedbandig storen

Door middel van breedbandige RF (*radio frequency*) *jamming* wordt de draadloze communicatie tussen drone en de piloot verstoord¹⁷. Het doel hiervan is dat de piloot de controle over de drone verliest waardoor in veel gevallen de drone terugkeert naar de Rth (*return to home*)-locatie¹⁸. Een nadeel van deze methode is dat ongewenste neveneffecten kunnen optreden omdat gestoord wordt in de volle breedte van de frequentiebanden waarin een drone of een drone *swarm* actief kan zijn.

3.3.2 Selectief storen

Deze selectievere vorm van RF jamming houdt in dat de draadloze communicatie-eigenschappen van een specifieke drone worden herkend en dat alleen deze worden verstoord. De drone ontvangt geen nieuwe instructies meer. Afhankelijk van het type drone zal deze op zijn plaats blijven ‘hangen’ of terugkeren naar de bekende Rth-locatie. Het voordeel van deze methode is dat er nagenoeg geen interferentie is op signalen van andere gebruikers in dezelfde frequentieruimte is omdat alleen gestoord wordt op de communicatie van de drone zelf en niet op andere frequenties.

3.3.3 Geavanceerd/’slim’ storen

Er bestaan meerdere vormen van geavanceerd storen ofwel *smart jamming*. Een goed voorbeeld is *take-over*. Deze techniek houdt in dat als het ware op de draadloze communicatie tussen piloot en drone wordt ingebroken. Hierdoor is het mogelijk om de communicatie van de piloot naar de drone over te nemen en deze van andere commando’s te voorzien. Het effect hiervan is dat de piloot de verbinding kwijt raakt en dat de drone bijvoorbeeld via een specifieke route aan de grond gezet kan worden.

Zoals bij selectief storen is het voordeel van deze methode dat er nagenoeg geen neveneffect is omdat alleen ingegrepen wordt op de communicatie van de drone zelf en niet op andere frequenties. Een ander voordeel is dat het hiermee mogelijk is om de drone op een vooraf bepaalde locatie te laten landen en vervolgens in beslag te nemen.

3.3.4 Misleiden

Misleiding via *spoofing* is een techniek waarmee de drone als het ware voor de gek gehouden wordt¹⁹ (daarmee zou take-over eveneens als spoofing beschouwd kunnen worden omdat de drone door het toesturen van andere instructies ook misleid wordt). In de meeste gevallen wordt met spoofing bij drones gesproken over het misleiden van de GNSS (Global Navigation Satellite System)-ontvanger. Hierdoor is de drone ‘in de veronderstelling’ heel ergens anders op de wereld te vliegen dan in werkelijkheid. Dit kan er

¹⁷ <https://doodlelabs.com/news/what-is-drone-jamming/>

¹⁸ <https://uavcoach.com/drone-jammer/>

¹⁹ <https://www.sciencedirect.com/science/article/pii/S2090447924000820>

bijvoorbeeld toe leiden dat de drone ‘denkt’ in een ‘verboden gebied’ te vliegen en daardoor de landing inzet of terugvliegt naar de RtH-locatie. Als de drone een UAV is en gebruikt maakt van een vooraf ingesteld vluchtplan, kan het effect zijn dat de drone ineens een hele andere kant opgaat omdat de locatie van de drone ineens afwijkt van het vluchtplan.

Een nadeel van deze techniek is dat gebruikers in de nabije omgeving ook dit GNSS-spoofing signaal ontvangen en daardoor ontregeld kunnen raken. Kanttekening hierbij is wel dat sommige drones een te grote afwijking in GNSS-positie kunnen detecteren en deze informatie dan alsnog negeren. Verder is een bekende oplossing tegen GNSS-spoofing het gebruik maken van de zogenoemde CRPA's (Controlled Reception Pattern Antennas)²⁰. Dit zijn antennes waarmee het mogelijk is om GNSS-signalen uit een onverwachte richting uit te doven, waardoor de betreffende GNSS-ontvanger het spoofing-signaal niet meer ontvangt en weer luistert naar het daadwerkelijke GNSS-signaal. Het gebruik van dit soort antennes maakt het algemeen lastiger om vanaf de grond te verstoren of te *spoofen*.

3.3.5 High Power Microwave

Met High Power Microwave (HPM) wordt een techniek bedoeld waarmee op afstand wordt ingegrepen op de juiste werking van elektronica van een drone in plaats van op de draadloze communicatie²¹. Hiervoor worden korte radiopulsen op zeer hoog vermogen (tot meerdere gigawatts) uitgezonden in een gerichte bundel²². Drones die zich in de bundel van een HPM-systeem bevinden zullen in veel gevallen hinder ondervinden en tot stoppen worden gedwongen. Voordeel van deze techniek is dat de eigenschappen van de gebruikte draadloze communicatie in de drone geen rol spelen; de effectiviteit van deze maatregel is hiervan niet afhankelijk. Nadeel van deze techniek is dat de apparatuur niet draagbaar is. Hoe dan ook zal extra aandacht besteed moeten worden aan de co-existentie met eigen systemen (de intra-Elektromagnetische Compatibiliteit (EMC)) en die met systemen van derden.

3.3.6 High Energy Laser

Een HEL zoals de in ontwikkeling zijnde voertuigmobiele Apollo van de Australische fabrikant EOS (Electro Optic Systems), is ontworpen om met een optisch vermogen van 150 kilowatt door secondenlange belichting een drone fysiek uit te schakelen²³. De inzet van een dergelijk hoog vermogen voor fysieke aangrijping heeft echter diverse nadelen, waaronder de lange aanstraalperiode, de vereiste koeling en logistiek en de hoge gevoeligheid van het effect voor atmosferische condities. In Nederland doet TNO onderzoek naar het potentieel van de inzet van HEL voor het aanbrengen van fysieke schade aan onder meer drones. Zoals gezegd kan HEL ook ingezet worden om optische drone-sensoren te verblinden of te verwarren. Voor deze soft-kill activiteit kan het benodigde vermogen een stuk lager zijn dan voor de hard-kill doelstelling. Hierdoor verminderen of vervallen een aantal van de juist genoemde bezwaren voor hard-kill maar vormt de selectie van de juiste golflengte een uitdaging.

²⁰ <https://www.spirent.com/blogs/crpa-antennas-explained-choosing-and-testing-the-best-anti-jam-solutions-for-gps-gnss-resilience>

²¹ <https://breakingdefense.com/2025/02/high-power-microwave-force-field-knocks-drone-swarms-from-sky/>

²² <https://www.emsopedia.org/entries/high-power-microwave-hpm/>

²³ *Lasers als wapen*, de Ingenieur, november 2025, blz. 13-17

3.4 Voorbeelden van incidenten

Het aantal incidenten met drones in Europa is recent wezenlijk gestegen en toont aan hoe belangrijk het is om hiertegen te acteren. In deze paragraaf wordt door een paar incidenten als voorbeeld te noemen, een beeld geschetst van de ernst van deze situatie. Hierbij is zeker geen compleetheid nagestreefd, te meer omdat deze selectie gemaakt is ten tijde van het schrijven van deze Monitorenditie en door de actualiteit ingehaald kan zijn.

3.4.1 Nationaal

In Nederland zijn meerdere drone-incidenten geweest zoals:

- Meldingen van een of meerdere drones boven de penitentiaire inrichting in Vught, de EBI (Extra Beveiligde Inrichting) in 2020 en 2024²⁴. Deze drones kunnen gebruikt worden voor smokkel, dropping van verboden spullen of voor spionage ten behoeve van ontsnappingspogingen²⁵. Dit incident heeft de discussie geopend of door de DJI (Dienst Justitiële Inrichtingen) zelf hard-kill acties tegen drones boven PI's (penitentiaire inrichtingen) mag worden uitgevoerd in plaats van door de politie²⁶. Op deze EBI is reeds een dronedetectiesysteem aanwezig. Daarnaast werkt men nauw samen met veiligheidspartners in de regio om eventuele drones zo snel mogelijk te signaleren;
- Tijdens de NAVO Summit in juni 2025 hebben verdachte drones gevlogen, voor zover bekend om foto's te nemen. De Koninklijke Marechaussee heeft het droneverbod tijdens dit event gehandhaafd²⁷ en heeft een Counter-Unmanned Aircraft Systems (C-UAS)-eenheid van Defensie de nodige drones onderschept na detectie door speciale Squire-radars en specifieke infraroodkijkers²⁸. Vervolgens zijn er door mobiele C-UAS-teams (zie Figuur 2) diverse softkill-opties toegepast om de drones te neutraliseren²⁹;



Figuur 2: Leden van een mobiel Counter Unmanned Aircraft Systems team tijdens de NAVO Summit 2025 [bron: Ministerie van Defensie]

²⁴ <https://beveiligingnieuws.nl/verdachte-drones-boven-pi-vught/>

²⁵ <https://nos.nl/artikel/2586820-luchtruim-boven-gevangenis-vught-permanent-gesloten>

²⁶ <https://dtvnieuws.nl/nieuws/artikel/drones-boven-pi-vught-in-de-toekomst-mogelijk-meteen-uit-de-lucht-halen>

²⁷ <https://www.marechaussee.nl/actueel/nieuws/2025/06/22/koninklijke-marechaussee-handhaaft-droneverbod-rondom-luchthavens-tijdens-novo-top>

²⁸ <https://www.defensie.nl/actueel/nieuws/2025/06/25/militairen-haalden-drones-boven-den-haag-uit-de-lucht>

²⁹ https://magazines.defensie.nl/landmacht/2025/09/02_counterdrone-aaaaad

- Onlangs, eind november 2025, zijn meerdere drones boven Eindhoven Airport en vlieg-basis Volkel waargenomen³⁰. Door tegenmaatregelen vanaf de grond zijn deze verdreven.

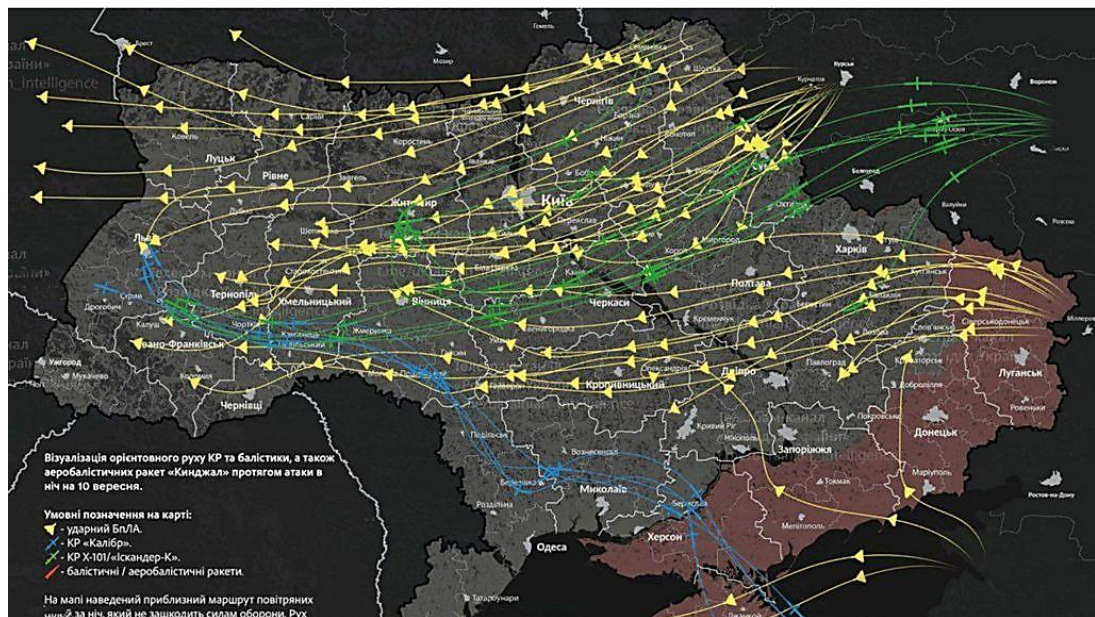
3.4.2 Duitsland

Volgens zowel Amerikaanse als Westerse bronnen hebben Russische verkenningsdrones eind augustus 2025 gevlogen over routes in Duitsland die door de Verenigde Staten worden gebruikt om militaire goederen te vervoeren naar onder meer Oekraïne. Deze drones lijken vooral ingezet voor het verzamelen van inlichtingeninformatie³¹.

Begin oktober 2025 zijn verdachte drones gespot in Noord-Duitsland bij de grens met Denemarken. Deze drones vlogen over belangrijke gebouwen en terreinen. In een gelekt memo wordt vermeld dat de drones vlogen in een “dronenetwerk met een moederdrone”. Deze drones leken in een parallelle vlucht het gebied en “kritieke infrastructuur” in kaart te brengen³².

3.4.3 Polen

UAV's zijn in september 2025 het Poolse luchtruim ingekomen door opzet of door effectieve tegenmaatregelen van Oekraïne, zoals GNSS-spoofing. Een aantal UAV's zijn door middel van hard kill, met F35-jachtvliegtuigen, uitgeschakeld³³.



Figuur 3: De banen van UAV's boven Oekraïne richting Polen in september 2025 [bron: X/@Podolyak_M]

Volgens de kaart in Figuur 3 betreft het in dit geval UAV's van Iraanse makelij en wel van het type Shahed.

Medio oktober 2025 is hinder door drones ondervonden door Nederlandse militairen in Polen, specifiek uitval van communicatie tijdens de NAVO-oefening *Falcon Autumn*³⁴.

³⁰ <https://www.defensie.nl/actueel/nieuws/2025/11/22/optreden-tegen-drones-boven-vliegbasis-volkel>

³¹ <https://nos.nl/artikel/2580290-russische-drones-vliegen-over-duitsland-en-bespioneren-wapenroutes-vs>

³² <https://nos.nl/artikel/2584784-verdachte-drones-vlogen-in-duitsland-over-parlementsgebouw-en-marinebasis>

³³ <https://nos.nl/collectie/13965/artikel/2581960-russische-drones-boven-polen-dit-levert-rusland-zeeen-aan-informatie-op>

³⁴ <https://nos.nl/artikel/2586405-nederlandse-militairen-in-polen-gehinderd-door-onbekende-drones>

3.4.4 Denemarken

Eind september 2025 zijn drones in de buurt van en boven een militaire vliegbasis in Karup waargenomen. Er wordt gesproken over meerdere incidenten op verschillende locaties. Eerder die maand was de luchthaven van Kopenhagen urenlang gesloten omdat er meerdere drones waren gezien in de omgeving. Volgens de autoriteiten waren het professionele, vrij grote drones³⁵.

3.4.5 Noorwegen

In september 2025 zijn ook twee drones in de buurt van het vliegveld bij Oslo gesignaleerd³⁶.

3.4.6 België

Recent zijn er diverse drone-incidenten geweest in België. Zo zijn begin november 2025 meerdere drones waaronder grotere, professionele exemplaren waargenomen boven de luchtmachtbasis Kleine-Brogel in de buurt van de grens met Nederland. Op deze basis liggen Amerikaanse kernwapens opgeslagen en vanaf 2027 wordt Kleine-Brogel de thuisbasis van nieuwe F-35-jachtvliegtuigen³⁷.

Ook zijn in diezelfde periode rond de vliegvelden in Brussel en Luik drones waargenomen die hebben geleid tot de nodige overlast³⁸.

3.5 Wat gebeurt er bij nationale inzet van tegenmaatregelen?

De inzet van tegenmaatregelen in Nederland (en in het algemeen) kan gezien worden in het licht van:

- Voorbereiding op een mogelijke dronedreiging, bijvoorbeeld tijdens grootschalige geplande evenementen zoals Sail Amsterdam, de Dutch Grand Prix en de NAVO Summit, of om kritische objecten of -infrastructuur te beschermen en daarnaast
- In meer acute gevallen, wanneer lokaal een concrete dronedreiging ontstaat.

In de volgende paragrafen wordt nader ingegaan op deze aspecten.

3.5.1 Voorbereiding van de mogelijke inzet van tegenmaatregelen tegen drones

Het is van belang om voor een aantal kritische infrastructuren en -objecten van tevoren te bepalen wat het effect is van een tegenmaatregel zoals de inzet van een radiofrequente UAS-tegenmaatregel. Mocht een situatie zich voordoen waarin een dergelijke tegenmaatregel toegepast moet worden dan is het bekend welke gevolgen dit zou kunnen hebben en kunnen mitigerende en preventieve maatregelen worden genomen. Hierbij valt te denken aan het aanleggen van een tijdelijke veiligheidszone om het object in kwestie door het tijdelijk sluiten van het lokale luchtruim, het instellen van een permanente *no-fly*

³⁵ <https://nos.nl/artikel/2584217-opnieuw-drones-boven-denemarken-nu-boven-luchtmachtbasis>

³⁶ <https://nos.nl/artikel/2583673-luchthavens-kopenhagen-en-oslo-weer-open-na-urenlange-sluiting-door-drones>

³⁷ <https://nos.nl/artikel/2589092-belgische-politie-jaagt-in-de-grensstreek-al-dagen-op-spoekdrones>

³⁸ <https://www.dw.com/en/flights-resume-at-brussels-airport-after-drone-sightings/a-74620347#:~:text=Flights%20were%20suspended%20Tuesday%20evening%20at%20Brussels%20and,several%20such%20sightings%20across%20Europe%20in%20recent%20months>

zone, het vaststellen van terugvalopties voor hulpdiensten, het publiceren van gebruiksrestricties van radioapparatuur zoals mobiele telefoons of van de risico's en beperkingen, et cetera.

3.5.2 Overgaan tot inzet: wat mag volgens de AMvB?

Specifiek tegen de dronedreiging bestaat sinds 22 april 2025 een AMvB (Algemene Maatregelen van Bestuur), het *Besluit afwijkend gebruik frequentieruimte*^{39,40} waardoor in gevaarlijke situaties overheidsdiensten sneller en effectiever apparatuur voor anti-dronemaatregelen zoals in Paragraaf 3.3 besproken, kunnen inzetten.

Er worden eisen gesteld aan de apparatuur, de opleiding en vaardigheden van de bedienaars ervan en de conditie waaronder mag worden overgegaan tot het gebruik. Voor wat betreft dit laatste geldt dat *jammers* tegen drones alleen mogen worden ingezet als:

- De drone ook daadwerkelijk is waargenomen;
- Er een ernstige, acute en herkenbare dreiging voor de veiligheid bestaat;
- Er geen minder ingrijpende middelen beschikbaar zijn om de dreiging te beëindigen.

Tenslotte moet de inzet van de jammers zodanig zijn, dat andere belangrijke spectrumgebruikers zoals van mobiele netwerken of van hulpdiensten zo min mogelijk worden verstoord. Met name moet dit gelden voor de zogenoemde vitale processen, volgens de definitie van de NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid). Elke inzet moet dan ook zorgvuldig worden afgewogen voor wat betreft stralingsrichting, zendvermogen en de duur in relatie tot de dreiging en de (radio)omgeving.

Ook in preventieve zin, bijvoorbeeld bij geplande evenementen zoals de NAVO Summit in juni 2025 of bij de bewaking van gevoelige locaties, kan deze AMvB in principe worden toegepast. Hiermee wordt voorkomen dat voor iedere inzet van anti-drone-apparatuur een aparte ontheffing moet worden aangevraagd, wat de nodige vertraging tot gevolg zou hebben. Door de strenge eisen die hierboven zijn genoemd kan echter, bij preventieve inzet (anders dan voor training en opleiding), de situatie ontstaan waarin het denkbaar is dat eerder wordt teruggevallen op tijdelijke ontheffingen dan dat de AMvB wordt toegepast.

³⁹ Staatsblad 106, 2025

⁴⁰ <https://www.dronewatch.nl/2025/04/28/overheid-krijgt-ruimere-bevoegdheid-om-drones-te-verstoren-bij-dreiging/>

4 5G-implementatie: de huidige stand van zaken

4.1 Inleiding

In de najaarseditie van de draadloze monitor van 2022⁴¹ is ingegaan op de dekking van commercieel 5G. Toen werd aangegeven dat 5G voornamelijk werd gebruikt door de consumentenmarkt en dat het gebruik uitbleef in sectoren zoals de industrie, gezondheid, landbouw et cetera. Belangrijke redenen hiervoor waren het ontbreken van beschikbare 3,5 GHz-band en van 5G standalone (SA)-netwerken. Reden dus om een update te geven over de huidige commerciële 5G-dekking, zowel voor publieke- als voor privénetwerken in Nederland en de rest van de wereld.

In Paragraaf 4.2 wordt ingegaan op de huidige stand van zaken rondom 5G in Nederland, met een focus op de commercieel vrijgekomen 3,5 GHz-band. In Paragraaf 4.3 wordt gekeken naar de mondiale ontwikkelingen rondom 5G-netwerken, met aandacht voor 5G SA, netwerkelementen- in het bijzonder in relatie tot Open Radio Access Network (O-RAN) en de status van 5G-gebruikersapparaten zoals smartphones, routers, wearables et cetera.

4.2 5G in Nederland

4.2.1 De 3,5 GHz-band in gebruik

De drie mobiele netwerk operators (MNO's) in Nederland zijn momenteel KPN, Odido (voorheen T-mobile) en VodafoneZiggo (voorheen Vodafone). De MNO's hebben op 25 juni 2024 toegang gekregen tot de 3,5 GHz-band⁴² die essentieel zijn om te voldoen aan de beloftes van 5G om groei in dataverbruik mogelijk te maken. Deze frequenties zijn vanaf juli 2024 commercieel in gebruik genomen. De banden van 3,45-3,55 GHz (VodafoneZiggo), 3,55-3,65 GHz (Odido) en 3,65-3,75 GHz (KPN)⁴³ bieden elk 100 MHz aan bandbreedte en staan vast tot 2040.

4.2.2 Dekking en snelheid

Volgens het techplatform Tweakers⁴⁴ is sinds de inschakeling van de 3,5 GHz-band een downloadsnelheid van meer dan 1,4 Gbit/s mogelijk. Op dit moment zijn er in totaal 14.630 5G masten verspreid over heel Nederland⁴⁵. Hiervan zijn er 4965 van KPN, 4793 van Odido en 4872 van Vodafone. Van deze masten worden er respectievelijk 1602 (KPN), 4474 (Odido) en

⁴¹ TNO 2022 P12274, december 2022, blz. 12

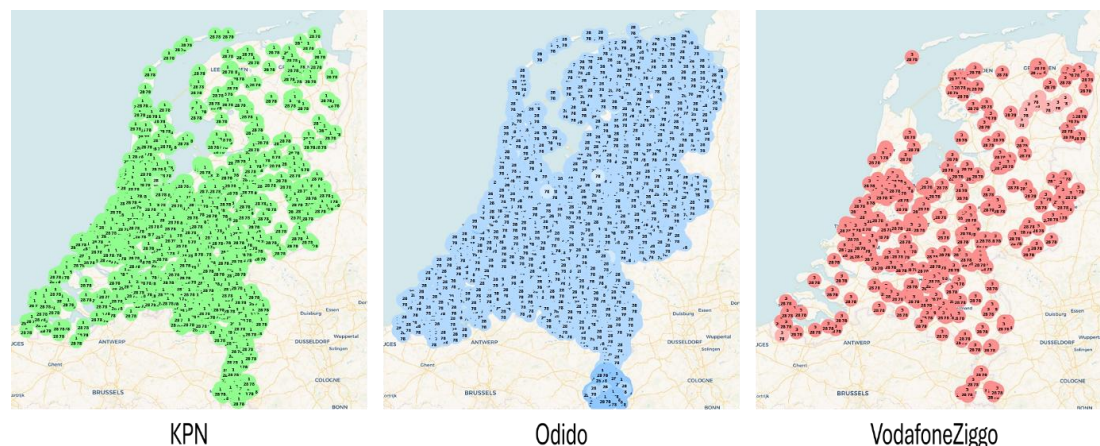
⁴² <https://www.rijksoverheid.nl/actueel/nieuws/2024/07/01/kpn-odido-en-vodafoneziggo-winnaars-veiling-nederlandse-5g-netwerken>

⁴³ <https://www.rdi.nl/actueel/nieuws/2024/07/01/kpn-odido-en-vodafoneziggo-verwerven-frequenties-via-5g-veiling>

⁴⁴ <https://tweakers.net/reviews/12812/5g-bereikt-volgende-fase-meer-capaciteit-in-nl-extra-aanbieder-in-be.html>

⁴⁵ <https://antennekaart.nl/>

584 (Vodafone) gebruikt voor de 3,5 GHz-band. In Figuur 4 is de huidige dekking van de 3,5 GHz-band voor de drie MNO's weergegeven.



Figuur 4: 5G-netwerkdekkingskaarten van de 3,5 GHz-band voor de drie Nederlandse MNO's per oktober 2025 [bron: antennekaart.nl]

Figuur 4 laat zien dat KPN vooral in Midden- en Zuid-Nederland dekking biedt, Odido vrijwel overal in Nederland dekking levert en VodafoneZiggo voornamelijk actief is in stedelijk gebied. Het aanzienlijk hiaat in dekking tussen Odido en de andere MNO's is opvallend. Odido zet sterk in op de 3,5 GHz-band en realiseert daarmee on-demand 5G⁴⁶ en internet aan huis (Klik&Klaar)⁴⁷. Dat laatste is uniek, omdat Odido op deze manier de concurrentie aangaat met vaste netwerk operators zoals Ziggo en DELTA. Volgens het RDI (Rijksinspectie Digitale Infrastructuur) blijft de uitrol van de 26 GHz-band voorlopig uit⁴⁸. Uit een recent rapport dat is opgesteld in opdracht van het Ministerie van Economische Zaken⁴⁹ blijkt dat er de komende jaren waarschijnlijk geen extra spectrum nodig zal zijn omdat het mobiele dataverbruik daarvoor niet snel genoeg toeneemt.

De huidige netwerken maken nog gebruik van non-standalone (NSA) 5G. Een 5G NSA-netwerk maakt deels gebruik van het bestaande 4G- ofwel LTE (Long Term Evolution)-netwerk om de verbinding op te zetten. Dit betekent dat het 5G-netwerk nog niet volledig zelfstandig functioneert, zoals de term al impliceert.

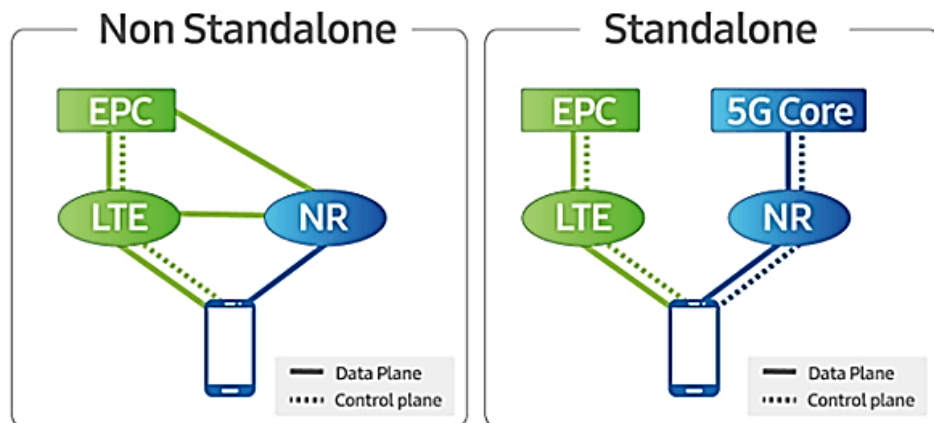
Er wordt gebruik gemaakt van 5G New Radio (NR) om data naar- en van de gebruiker te versturen. Dit maakt het onder andere mogelijk dat telefoons die geschikt zijn voor 5G-gebruik kunnen maken van hoge datasnelheden op andere frequentiebanden. Figuur 5 laat het verschil tussen 5G SA en 5G NSA zien.

⁴⁶ <https://newsroom.odido.nl/odido-lanceert-simwallet-on-demand-5g-internet-voor-iedereen-in-nederland-dankzij-nieuwe-app/>

⁴⁷ <https://www.odido.nl/>

⁴⁸ <https://www.rdi.nl/onderwerpen/dossier-5g/frequenties>

⁴⁹ <https://www.rijksoverheid.nl/documenten/rapporten/2025/09/30/future-trends-in-radio-frequency>



Figuur 5: De vergelijking tussen een 5G NSA en 5G SA network. In groen het bestaande LTE netwerk en in blauw het 5G netwerk [bron: www.everythingrf.com]

Figuur 5 geeft aan dat een 5G SA-netwerk zowel dataverkeer als controleberichten via een op zichzelf staand netwerk laat verlopen. In tegenstelling tot 5G NSA worden de controleberichten dus niet meer via het 4G-netwerk verstuurd. Door het gebruik van een 5G SA-netwerk zijn verbeteringen mogelijk op het gebied van vertraging (*latency*) en wordt het mogelijk om gebruik te maken van *network slicing*. Daarbij wordt één fysiek 5G-netwerk opgedeeld in meerdere virtuele netwerken (*slices*), waarbij elke slice afzonderlijk kan worden geconfigureerd voor een specifieke dienst⁵⁰. Zo kan bijvoorbeeld één slice worden ingezet voor hoge datasnelheden, terwijl een andere slice juist is geoptimaliseerd voor minimale vertraging.

De uitrol van 5G SA laat ook ten tijde van het schrijven van deze najaarseditie van 2025 nog op zich wachten. Vanwege hoge investeringen in voorzieningen voor 5G SA lijken MNO's grote zorgvuldigheid te betrachten bij de uitrol van SA, waarbij business cases voor lage latentie en *network slicing* overtuigend genoeg moeten zijn om deze investeringen te rechtvaardigen.

In de tussentijd zijn er wel testen uitgevoerd met een 5G SA-netwerk. In 2024 heeft KPN, in samenwerking met logistiek dienstverlener KLG Europe, testen gedaan met een privé 5G SA-netwerk⁵¹. Deze test liet zien dat er met een lokaal netwerk een vertraging van 4 ms gehaald kon worden. Ter vergelijking, met het huidige 5G NSA-netwerk wordt een vertraging van ongeveer 18 ms behaald⁵². Van de privénetwerken in Nederland wordt momenteel 50% met 5G-technologie ingezet⁵³. Daarbij wordt geen onderscheid gemaakt tussen SA- en NSA-5G-netwerken. Verder heeft KPN in 2023, in samenwerking met Ericsson, een *cloud gaming* test opgezet waarin gebruik is gemaakt van de 3,5 GHz-band. Tijdens deze test kon de gebruiker in real-time een online game spelen via meerdere masten in de buurt⁵⁴. Hier zijn datasnelheden behaald van 1 Gbit/s en is een vertraging van 14 ms gemeten. Er zijn momenteel geen bekende ontwikkelingen bij Odido en VodafoneZiggo met betrekking tot een 5G SA-netwerk.

Naast de nieuwe frequentiebanden werken de drie MNO's ook aan het verbeteren van hun netwerkcomponenten. De grootste verandering is de inzet van *beamforming* en MIMO (Multiple Input Multiple Output). Met beamforming kun je nauwkeurige bundels maken die

⁵⁰ Xiaoyang, "What Is Network Slicing?" Huawei, July 1, 2021. <https://info.support.huawei.com/info-finder/encyclopedia/en/Network+Slicing.html>

⁵¹ <https://www.overons.kpn/nieuws/kpn-zet-volgende-stap-met-5g/>

⁵² <https://tweakers.net/reviews/9324/bereik-en-prestaties-op-5g-netwerk-getest.html>

⁵³ *Private Mobile Networks, June 2025. GMSA summary*

⁵⁴ <https://www.overons.kpn/nieuws/en/kpn-is-taking-the-next-step-in-5g-development/>

gericht data van- en naar de gebruiker kan zenden in plaats van deze in alle richtingen uit te zenden. Met MIMO worden meerdere antennes ingezet als afzonderlijke dataverkeerkanalen, waardoor meer gegevens tegelijk verzonden kunnen worden. Medio 2024 is Odido begonnen met het verbeteren van haar zendmasten door het implementeren van zowel beamforming als MIMO⁵⁵. Dit verhoogt de capaciteit van het netwerk, omdat er tegelijkertijd meerdere datastromen gezonden kunnen worden en in het geval van MU (Multi User)-MIMO ook naar meerdere gebruikers.

4.2.3 5G-gebruikersapparaten en -netwerkelementen

In Nederland kun je momenteel kiezen uit minstens negen fabrikanten van 5G-ready gebruikerstoestellen. Hieronder vallen bekende smartphonemerken zoals Apple, Samsung en Google, maar ook de Chinese merken OPPO, Xiaomi en OnePlus, evenals speciale merken als Fairphone (met het oog op duurzaamheid). Ook bieden Motorola en Nokia (vallend onder HMD) diverse 5G-gebruikersapparaten aan. Huawei is nagenoeg afwezig in het 5G-segment in Nederland, mede door de handelsbeperkingen die op het bedrijf van toepassing zijn⁵⁶. Sinds de Monitor-najaarseditie van 2022 is volgens een smartphonevergelijking op Tweakers het aantal 5G-ready gebruikerstoestellen in Nederland gegroeid naar in totaal 1.284.

Naast de Klik&Klaar-oplossing van Odido, zoals genoemd in Paragraaf 4.2.2, zijn er momenteel ook mobiele 5G hotspots en 5G-ready tablets op de markt. Een vergelijking van 5G-Mifi (mobiele Wi-Fi) apparaten leverde 10 apparaten op waarmee je een 5G-hotspot kunt creëren. Daarnaast worden ook tablets uitgerust met 5G. Specifiek bieden Apple, Samsung en Microsoft tablettoestellen aan die 5G-ready zijn.

De drie MNO's hebben elk hun eigen keuzes gemaakt in netwerkleveranciers voor de RAN- en de core-netwerken. Deze keuzes zijn beïnvloed door technologische prestaties maar ook door geopolitieke factoren. Sinds begin 2024 maakt KPN voor het RAN-gebruik van basisstations van Huawei⁵⁷. Voor het core-netwerk is bewust gekozen voor Ericsson⁵⁸ vanwege de eis vanuit de Nederlandse overheid om vertrouwde (westerse) leveranciers te gebruiken in kritieke onderdelen van het netwerk. In de zomer van 2022 heeft Odido zowel het RAN als het core-netwerk volledig ondergebracht bij Ericsson⁵⁹. VodafoneZiggo werkte al nauw samen met Ericsson en heeft in het najaar van 2025 aangekondigd dit te verlengen met een vijfjarig partnerschap op het gebied van 5G⁶⁰.

4.3 5G in de rest van de wereld

4.3.1 Milde uitrol van SA 5G met China als koploper

In 2025 zijn er wereldwijd investeringen door MNO's gedaan om 173 publieke 5G SA-netwerken te realiseren⁶¹. Dit aantal staat tegenover een totaal van 639 5G-netwerken. Dat betekent dat momenteel 27% van alle 5G-netwerken een 5G SA-netwerk is. Niet alle netwerken worden direct commercieel ingezet. Van de 173 5G SA-netwerken zijn er 77 gelanceerd, wat neerkomt op 44,5%. Voor de overige netwerken worden veldtesten uitgevoerd of staan ze nog gepland voor lancering. In vergelijking met de draadloze monitor

⁵⁵ <https://tweakers.net/reviews/12006/beamforming-en-mu-mimo-5g-krijgt-upgrade.html>

⁵⁶ <https://tweakers.net/reviews/7518/huawei-raakt-verstrikt-in-wereldpolitiek.html>

⁵⁷ <https://antennekaart.nl/>, "KPN rondt Huawei migratie af, begint met uitrol 3500MHz."

⁵⁸ <https://www.ericsson.com/en/press-releases/2020/10/kpn-netherlands-selects-ericsson-for-5g-core>

⁵⁹ "T-Mobile zet eerste honderd masten om naar Ericsson.", <http://www.odido.nl/>

⁶⁰ <https://www.ericsson.com/en/press-releases/2025/10/ericsson-and-vodafone-announce-major-five-year-programmable-networks-partnership>

⁶¹ *5G Standalone August global status update*, Global mobile Suppliers Association, August 2025, blz. 2

van het najaar 2022 is het aandeel 5G SA ten opzichte van alle 5G-netwerken slechts met 5% gegroeid.

Verder laat Ookla, de organisatie die onder andere testen voor downloadsnelheden verzorgt, zien dat China, India en de Verenigde Staten vooroplopen in het aanbieden van 5G SA⁶². Eind 2024 had ruim 80% van de Chinese gebruikers, meer dan 50% van de gebruikers in India en meer dan 20% van de gebruikers in de Verenigde Staten een 5G SA-verbinding opgezet. De hoge inzet door China is te herleiden tot de verplichting die de Chinese overheid sinds 2020 heeft opgelegd, waarbij alle 5G-gebruikersapparaten voortaan 5G SA moeten ondersteunen⁶³. Sinds 2021 zijn zowel nieuwe als bestaande netwerken in China standaard ingesteld op 5G SA.

Aan het einde van het derde kwartaal van 2024 had 15% van de MNO's in Europa een werkend 5G SA-netwerk⁶⁴. Verder vermeldt Ookla dat in Europa slechts 2% van de mobiele apparaten gebruik maakt van 5G SA, ten opzichte van alle 5G-netwerken⁶⁵. Dit wekt de suggestie dat in Europa voornamelijk gebruik wordt gemaakt van 5G NSA voor het publiekelijk netwerk. Als 5G SA wordt gebruikt dan is dat vooral voor privénetwerken.

Wereldwijd zijn er in totaal 1.846 privé mobiele netwerken, waarvan 28,5% gebruik maakt van 5G SA⁶⁶. Daarbij moet opgemerkt worden dat het merendeel van deze netwerken wordt gebruikt door onderwijsinstellingen of validatiecentra, wat erop kan wijzen dat het 5G SA-netwerk zich nog in de ontwikkelingsfase bevindt of dit vanuit een commercieel oogpunt nog niet interessant genoeg is. Verder worden volgens de GSA de 5G-privénetwerken ook ingezet voor sportevenementen, financiële diensten (zoals banken) en ziekenhuizen⁶⁷.

4.3.2 5G mobiele gebruikersapparaten en netwerkelementen

Volgens de GSA zijn er in juni van dit jaar bijna 3.500 mobiele 5G gebruikersapparaten aangekondigd⁶⁸, waarvan 71,4% geschikt is voor 5G SA en het overige deel voor 5G NSA. Van die SA mobiele apparaten is ongeveer 90% al commercieel beschikbaar. De frequentiebanden waarin deze 5G SA-mobiele apparaten functioneren zijn volgens de GSA voornamelijk 700 MHz, 3,5 GHz en 26 GHz en zijn niet veranderd ten opzichte van de editie draadloze monitor van het najaar 2022. Wel is in drie jaar tijd het aantal millimetergolf chipsets gegroeid van drie naar 16 stuks. Deze chipsets zijn afkomstig van onder andere Qualcomm, Samsung, NEC, Fujitsu en Mediatek. In Europa zijn Benetel en Acceleran actief. De millimetergolf technologie is meestal geïmplementeerd als een modem of RF-sub-systeem dat gekoppeld is aan de chipset.

De nieuwste modems van Qualcomm die compatibel zijn met de Snapdragon-lijn, de X75 en X80, zijn bijvoorbeeld te vinden in de Samsung Galaxy S24 en de iPhone 17 Pro⁶⁹. Samsung heeft een verrassende stap gezet door een millimetergolfchipset te integreren in de Google

⁶² https://www.ookla.com/s/media/2025/02/ookla_omdia-5GSA_0225b.pdf, blz. 2

⁶³ Ericsson.Com, "5G Standalone Deployment: Moving beyond eMBB.", <https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/5g-standalone-deployment>

⁶⁴ *The Mobile Economy Europe 2025*. Global mobile Suppliers Association, 2025

⁶⁵ https://www.ookla.com/s/media/2025/02/ookla_omdia-5GSA_0225b.pdf, blz. 16

⁶⁶ *Private Mobile Networks Summary, September 2025*. Global Mobile Suppliers Association summary

⁶⁷ *Private Mobile Networks Summary, June 2025*. Global Mobile Suppliers Association summary

⁶⁸ *5G Standalone August global status update*, Global mobile Suppliers Association, August 2025, blz. 4

⁶⁹ <https://www.qualcomm.com/5g/mmwave>

Pixel Pro 6⁷⁰. Mediatek heeft de Dimensity 1050 uitgebracht, die onder andere te vinden is in de Motorola Edge 2022⁷¹.

Op het gebied van nieuwe netwerkelementen voor het 5G-netwerk zijn er stappen gezet in O-RAN (zie Hoofdstuk 5). Met O-RAN is het voor MNO's mogelijk om gebruik te maken van verschillende apparatuur, die onderling goed samenwerkt, bij het opzetten van het mobiele netwerk⁷². Bij traditionele RAN zijn de MNO's afhankelijk van één leverancier voor het volledige RAN systeem, zoals Ericsson of Huawei, wat de keuzevrijheid in apparatuur en diensten beperkt. Hierbij wegen de operators het risico van *vendor lock-in* af tegen de complexiteit van het integreren van losse onderdelen in een netwerk. Sinds mei 2025 bestaat 5 tot 10% van de totale RAN markt uit O-RAN en de verwachting is dat dit aandeel zal groeien naar 30% in 2028⁷³. Meer over de ontwikkeling van O-RAN is te lezen in Hoofdstuk 5.

.

⁷⁰ <https://www.everythingrf.com/news/details/13697-samsung-makes-a-surprise-entrance-in-the-5g-mmwave-chipset-market-to-compete-with-qualcomm>.

⁷¹ <https://www.mediatek.com/press-room/mediatek-launches-first-mmwave-chipset-for-seamless-5g-smartphone-connectivity>

⁷² <https://www.nokia.com/mobile-networks/ran/anyran/open-ran/open-ran-explained/>

⁷³ <https://www.firstpointgroup.com/resources/blog/open-ran-market-update/>

5 Open RAN: voortgang en perspectieven

5.1 Introductie

De Open RAN Alliance werd in 2018 opgericht door toonaangevende, wereldwijde operators met de visie om de Radio Access Network (RAN)-industrie te transformeren tot een meer open en doordacht, gevirtualiseerd en volledig interoperabel ecosysteem. Dit initiatief was revolutionair in een tijd waarin RAN een gesloten, door leveranciers gecontroleerde *black box* was. In de afgelopen zeven jaar heeft deze Alliance drie belangrijke releases gepubliceerd, met specificaties voor architectuur, interfaces, 'cloudificatie' en beveiliging. De voorjaarseditie uit 2021⁷⁴ belichtte de vroege adoptiefase, de huidige editie bespreekt in dit hoofdstuk de belangrijkste voortgang die sindsdien heeft plaatsgevonden. Als toelichting op de technische achtergrond en begrippen van O-RAN wenselijk mocht zijn, kunnen deze gevonden worden in Paragraaf 2.5 van de voorjaarseditie van 2021.

In 2021 won Open RAN (O-RAN) aan populariteit onder operators en leveranciers. De O-RAN-technologie splitst het traditionele, geïntegreerde RAN waar hardware en software nauw met elkaar verbonden waren, op in modulaire softwarecomponenten die op generieke hardware draaien. Open interfaces maken interoperabiliteit mogelijk, waardoor componenten van verschillende leveranciers kunnen samenwerken. De meeste implementaties bevonden zich in deze tijd echter nog in de test- of vroege commerciële fase en het O-RAN-ecosysteem werd gedomineerd door een paar grote leveranciers. De eerste commerciële lanceringen hadden net plaatsgevonden in Japan, Italië en Peru en de industrie was optimistisch maar voorzichtig, met zorgen over de mate van ontwikkeling ('volwassenheid') van O-RAN, prestaties en beveiliging.

5.2 Belangrijke ontwikkelingen sinds 2021: marktacceptatie en -implementatie

Sinds 2021 heeft O-RAN een snelle groei met belangrijke mijlpalen doorgemaakt. In Paragraaf 5.2.1 wordt eerst toelichting gegeven op de ontwikkelingen die ondersteunend zijn aan de marktpositie en gebruiksgroei van O-RAN. Vervolgens gaat Paragraaf 5.2.2 specifiek in op de eigenlijke, kwantitatieve marktontwikkeling.

5.2.1 Ontwikkeling van O-RAN-ondersteuning

In deze paragraaf worden twee ontwikkelingen besproken die belangrijk waren en zijn voor de stimulering van het gebruik van O-RAN: de uitbreiding van Open Testing and Integration Centers (OTIC's) en de invloed van Open Cloud (O-Cloud).

⁷⁴ TNO 2021 R10974, juni 2021, blz. 39-45

5.2.1.1 De uitbreiding van OTIC's

Een OTIC is een leveranciersonafhankelijk, open en onpartijdig laboratorium dat de voortgang van het O-RAN-ecosysteem ondersteunt en als zodanig door de O-RAN Alliance is erkend. Deze OTIC's bieden samenwerkingsomgevingen voor conformiteit, interoperabiliteit en *end-to-end*-testen van O-RAN-oplossingen en -producten. Ze zijn bevoegd om O-RAN-certificaten en -badges⁷⁵ uit te reiken en organiseren *plugfests*: internationale test- en integratie-evenementen om de ontwikkeling van daadwerkelijk open en interoperabele O-RAN te bevorderen. Specifiek bieden OTIC's referentieopstellingen en testbeds aan voor het valideren van interoperabiliteit tussen meerdere leveranciers. Dit zorgt ervoor dat O-RAN-componenten van verschillende leveranciers goed samenwerken voordat ze in actieve netwerken worden geïmplementeerd. Het aantal OTIC's is wereldwijd gegroeid van slechts twee naar meer dan 20, waaronder negen in de Verenigde Staten, vijf in Europa (Berlijn, Madrid, Parijs, Turijn, Londen), zeven in Azië en één in Zuid-Amerika⁷⁶.

De regelmatige plugfests en testen hebben de interoperabiliteit wezenlijk verbeterd en zijn hierdoor meer volwassen producten ontstaan en betere ondersteuning voor geavanceerde functies zoals Massive MIMO (Multiple Input Multiple Output) en mmWave. De sector is overgestapt van de oorspronkelijke zogenoemde *greenfield*-implementaties waarin geen beperkingen door bestaande netwerken werden ervaren, naar de inpassing van O-RAN in *brownfield*-netwerken, waarmee de integratie met bestaande netwerken bewust is gerealiseerd. Hiermee is de O-RAN sector in principe klaar voor grootschalige commerciële implementatie.

5.2.1.2 De rol van O-Cloud

O-Cloud is een fundamenteel onderdeel van de O-RAN-architectuur. Deze is ontworpen om een *cloud-native* platform te bieden voor het hosten en automatiseren van RAN-functies. In tegenstelling tot traditionele telecom hardware is O-Cloud geen enkel apparaat maar een gedistribueerde set *resource pools*: CPU's (Central Processing Units), geheugen, opslag, netwerkinterfaces en processing accelerators zoals FPGA's (Field Programmable Gate Arrays) of GPU's (Graphics Processing Units). De resource pools zijn verspreid over gecentraliseerde en *edge*-locaties. Deze infrastructuur ondersteunt de implementatie van O-RAN centrale eenheden (Central Units- CU's), gedistribueerde eenheden (Distributed Units- DU's)⁷⁷, beheer- en orkestratielagen en observatiefuncties die alle de flexibiliteit en schaalbaarheid van *cloud computing* bieden.

O-Cloud stelt operators in staat om netwerkfuncties uit te voeren als *virtual machines* of *containers* die nauw zijn geïntegreerd met orkestratieplatforms. Hierdoor wordt geautomatiseerde schaalbaarheid, netwerkisolatie en real-time beheer van de netwerkbelasting mogelijk. Geavanceerde functies worden ondersteund zoals hardware-versnelling, pakket-I/O (Input/Output) met lage vertraging en nauwkeurige tijdsynchronisatie, die essentieel zijn voor de prestaties van moderne mobiele netwerken. Door via O-Cloud gestandaardiseerde infrastructuurbeheer- en levenscyclus-diensten te bieden, kunnen operators oplossingen van meerdere leveranciers integreren, netwerkprestaties optimaliseren en AI-gestuurde automatisering toepassen binnen het RAN. Hierdoor kunnen mobiele 5G en 6G-netwerken sneller aanpasbaar, kosten-effectiever en robuuster worden.

⁷⁵ <https://www.o-ran.org/certification-badging>

⁷⁶ <https://www.o-ran.org/otic>

⁷⁷ TNO 2021 R10974, juni 2021, blz. 40

5.2.2 Ontwikkeling van de O-RAN markt

Zoals aangegeven in Hoofdstuk 4, wordt verwacht dat het aandeel van O-RAN van de totale RAN-markt zal groeien van de huidige 5 tot 10% naar 30% in 2028. Ook in absolute zin is de O-RAN-markt snel gegroeid en werd in 2025 gewaardeerd op circa \$ 3 miljard. Naar verwachting zal deze in 2034 ruim \$ 38 miljard bereiken, met een samengesteld jaarlijks groeipercentage (CAGR: Compound Annual Growth Rate) van meer dan 32%.

Noord-Amerika is koploper in marktaandeel door uitgebreide 5G-implementaties, regelgevende ondersteuning en sterke investeringen in telecommunicatie-infrastructuur. De sterkste groei is te verwachten van Azië-Pacific door toedoen van de voortvarende 5G-implementatie en de grote vraag naar flexibele en kosteneffectieve oplossingen^{78,79}.

Vijf grote MNO's in Europa (Deutsche Telekom, Orange, Vodafone, Telefónica en Telecom Italia) zijn een samenwerking aangegaan om de ontwikkeling van O-RAN te versnellen⁸⁰. Zo is Deutsche Telekom een samenwerking gestart met Nokia om 3.000 O-RAN-netwerken in Duitsland op te zetten⁸¹. Vodafone heeft Samsung geselecteerd voor het leveren van O-RAN randapparatuur en software⁸². Een van de grote MNO's in de Verenigde Staten, AT&T, streeft ernaar dat in 2026 70% van het netwerk, dat wordt opgezet in samenwerking met Ericsson en 1Finity, op O-RAN zal draaien⁸³. Voorlopers in het gebruik van O-RAN in Azië zijn Japan, Singapore, Cambodja, Indonesië en de Filipijnen, gedreven door OREX (O-RAN Ecosystem Experience)⁸⁴.

Het ledenaantal van de O-RAN Alliance is aanzienlijk gegroeid, met actieve deelname van traditionele leveranciers zoals Nokia en Ericsson maar ook met nieuwe partijen waaronder Mavenir, Altiostar en Parallel Wireless. Figuur 6 geeft een beeld van de betrokken partijen (leveranciers en operators) in het O-RAN-ecosysteem.

Rakuten Mobile in Japan is een treffend voorbeeld van een O-RAN *flagship*, met een volledig gevirtualiseerd 5G-netwerk, gebaseerd op O-RAN. Dell heeft zijn focus verlegd, wat de groeiende behoefte aan kan geven aan systeemintegratoren die integrale netwerkimplementaties van meerdere leveranciers kunnen realiseren. Hierbij moet worden aangetekend dat de meeste O-RAN *deployments* nog *single vendor* zijn, met name de CU en DU met koppeling van Radio Units (RU's) die van verschillende leveranciers kunnen zijn.

⁷⁸ <https://www.precedenceresearch.com/open-ran-market>

⁷⁹ <https://www.globenewswire.com/news-release/2025/04/11/3060132/0/en/Open-RAN-Market-Poised-to-Reach-USD-41-5-Billion-by-2032-Driven-by-Demand-for-Network-Flexibility-and-Cost-Efficiency-SNS-Insider.html>

⁸⁰ [ran.org/blog/open-rans-global-momentum/](https://www.ran.org/blog/open-rans-global-momentum/)

⁸¹ *Bloomberg.Com*, November 27, 2024. <https://www.bloomberg.com/news/articles/2024-11-27/deutsche-telekom-ramps-up-open-network-deal-with-nokia>

⁸² <https://www.samsung.com/global/business/networks/insights/blog/0930-samsung-selected-by-vodafone-to-provide-virtualized-ran-and-open-ran-solutions-across-europe/>

⁸³ <https://www.rcrwireless.com/20250805/carriers/att-ericsson-open-ran>

⁸⁴ Dyer, “(Another) New Dawn Breaks to the East for Open RAN.” *The Mobile Network*, November 6, 2024. <https://the-mobile-network.com/2024/11/another-new-dawn-breaks-to-the-east-for-open-ran/>



Figuur 6: Overzicht van actieve partijen in het O-RAN ecosysteem [bron: John Baker]

Private netwerken zoals in fabrieken en kantoren en implementaties op het platteland waren *early adopters*; grotere openbare netwerken gebaseerd op O-RAN zijn nu als *next big step* te verwachten.

5.3 Voortgang in standaardisatie

Specificaties voor open interfaces en nieuwe componenten zijn inmiddels volwaardig geworden. Voortdurend zijn er updates om beveiliging, prestaties en de cloud-integratie te verbeteren.

In augustus 2024 ondertekenden de O-RAN Alliance en ATIS (Alliance for Telecommunications Industry Solutions) een Memorandum of Understanding (MoU) om de O-RAN-specificaties om te zetten in Noord-Amerikaanse standaarden, hetgeen de wereldwijde acceptatie verder bevordert.

Vooruitlopend op 6G heeft eind 2023 de O-RAN next Generation Research Group (nGRG) een eerste rapport geschreven over de aansluiting van O-RAN op de aspecten van 6G⁸⁵. Hierin werd onder meer vastgesteld dat de ORAN-architectuur en -specificaties gebaseerd moeten zijn op gemeenschappelijke 3GPP-standaarden. In april 2025 werd de eerste gezamenlijke 6G workshop tussen O-RAN Alliance en 3GPP gehouden rondom betere afstemming tussen de twee organisaties om compatibiliteit te garanderen en dubbel werk te voorkomen⁸⁶. Dit geldt voor gebieden zoals de toepassing van AI/ML in alle netwerkdomeinen, 6G fronthaul (de interface tussen radio units en baseband units), *cloudnative* technologie, *digital twins* en 'softwarisedising'. Specifiek heeft 3GPP tijdens de RAN *plenary* van september 2025 een *Way forward on 6G fronthaul* gedefinieerd, waarbij de radio unit als logisch onderdeel van de 6G basisstation-architectuur mee is genomen⁸⁷.

De daadwerkelijke afstemming van het gedachtegoed van de O-RAN Alliance en dat van de 3GPP blijkt in de praktijk echter lastiger dan aanvankelijk aangenomen, met name rond de Lower Layer Split (LLS) in de 6G-architectuur en het O-RAN's *open fronthaul* paradigma. Dit wil *vendor lock-in* reduceren maar heeft ook gevolgen voor de complexiteit in standaarden, terwijl dit laatste en marktfragmentatie doorgaans niet de voorkeur hebben van operators⁸⁸.

⁸⁵ https://mediastorage.o-ran.org/ngrg-rr/ngrg-rr-2023-01-O-RAN-Towards-6G-v1_3.pdf

⁸⁶ https://www.3gpp.org/ftp/workshop/2025-04-24_3GPP_ORAN_JWS/Docs/3ORW-250035.zip

⁸⁷ https://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_109/Docs/RP-252881.zip

⁸⁸ <https://www.telecomtv.com/content/6g/why-there-are-no-guarantees-for-6g-open-ran-53599/>, augustus 2025

Hierdoor treedt het gevaar op van enigszins draconische compromissen waarvan de uitwerking bovendien veel tijd vergt.

Beveiliging is een centraal aandachtspunt geworden, waarbij de Security Working Group van de O-RAN Alliance de eisen en controles heeft verbeterd om te komen tot een *zero trust*-architectuur (ZTA). Dit omvat nieuwe beveiligings-test cases, dreigingsmodellering en risicobeoordeling, zodat O-RAN-systemen kunnen voldoen aan de verwachtingen van de industrie ten aanzien van veiligheid in combinatie met de openheid van O-RAN.

5.4 Uitdagingen en *lessons learned*

Ondanks de vooruitgang kampt O-RAN met technische en operationele uitdagingen. Er blijven zorgen bestaan over de beveiliging, met discussies over de vraag of openheid het risico vergroot of verkleint. De O-RAN Alliance heeft een Security Focus Group opgericht om deze problemen aan te pakken. Specifiek helpt de invoering van *zero-trust*-principes om kwetsbaarheden te beperken.

O-RAN-producten zijn nog steeds in ontwikkeling, waarbij sommige geavanceerde functies achterblijven bij traditionele RAN-oplossingen. Het gaat vooral om de schaalbaarheid en volwassenheid van producten.

Verder hebben de complexiteit die gemoeid is met integratie en de aanzienlijke behoefte aan bekwaame professionals in cloud-native architectures, software-gedefinieerde netwerken en cybersecurity geleid tot een tekort aan vaardigheden in de sector.

Rond interoperabiliteit en integratiecomplexiteit moet worden opgemerkt dat het bereiken van naadloze interoperabiliteit tussen diverse componenten een uitdaging kan zijn. O-RAN Alliance gaat deze uitdaging aan, met name in de testspecificaties die zijn opgesteld om de end-to-end-interoperabiliteit van de belangrijkste componenten van deze *multi-vendor* en idealiter *plug-and-play*-architectuur te valideren.

5.4.1 Greenfield of brownfield-implementaties?

Zoals eerder is aangegeven, verwijst *greenfield*-implementatie naar het vanaf nul opbouwen van een nieuw mobiel netwerk, zonder bestaande infrastructuur of beperkingen van leveranciers. Deze aanpak stelt operators in staat om O-RAN-principes volledig te omarmen, de beste componenten van meerdere leveranciers te selecteren, gebruik te maken van cloud-native architectures en de nieuwste standaarden en interfaces te implementeren zonder compatibiliteitsproblemen. Greenfield-implementaties zijn doorgaans sneller te innoveren en eenvoudiger te optimaliseren op basis van kosten en prestaties, zoals te zien is bij operators zoals Rakuten Mobile in Japan.

Brownfield-implementatie daarentegen omvat de integratie van O-RAN-technologieën in bestaande, *legacy*-netwerken. Dit scenario is complexer, omdat operators de interoperabiliteit tussen nieuwe O-RAN-componenten en oudere, 'bedrijfseigen' systemen moeten garanderen. Brownfield-implementaties vereisen een zorgvuldige planning om co-existent, migratie en operationele continuïteit te beheren, vaak met gefaseerde upgrades en hybride architectures. De uitdaging is om de voordelen van openheid en flexibiliteit te benutten en tegelijkertijd de betrouwbaarheid van de service te behouden en bestaande systemen (en dus investeringen) te benutten.

Early adopters van O-RAN melden voordelen op het gebied van flexibiliteit en kosten, maar benadrukken ook de noodzaak van robuuste integratie en ondersteuning. De overgang van greenfield- naar brownfield-implementaties vereist nieuwe strategieën voor het beheer van bestaande apparatuur en het garanderen van een goede operationele werking.

5.5 Voortgang rond beleid en regelgeving

Overheden en toezichthouders hebben een cruciale rol gespeeld bij het bevorderen van de acceptatie van O-RAN. In de Verenigde Staten heeft de National Telecommunications and Information Administration (NTIA) een Public Wireless Supply Chain Innovation Fund van \$ 1,5 miljard gelanceerd ter ondersteuning van open, interoperabele RAN-oplossingen. Het Verenigd Koninkrijk heeft een Open Networks Programme van £ 295 miljoen opgezet om de diversificatie van de toeleveringsketen te stimuleren met als doel om in 2030 35% van het mobiele netwerkverkeer via open netwerken te laten verlopen.

De beleidskaders ontwikkelen zich om open standaarden en interoperabiliteit te ondersteunen, waarbij de Amerikaanse en andere westerse overheden de acceptatie ervan stimuleren om de afhankelijkheid van risicovolle leveranciers te verminderen en innovatie te stimuleren. Regelgevende ondersteuning heeft de marktintroductie voor nieuwe leveranciers en integrators versneld en zal van positieve invloed zijn op een bredere acceptatie van O-RAN.

5.6 Conclusies

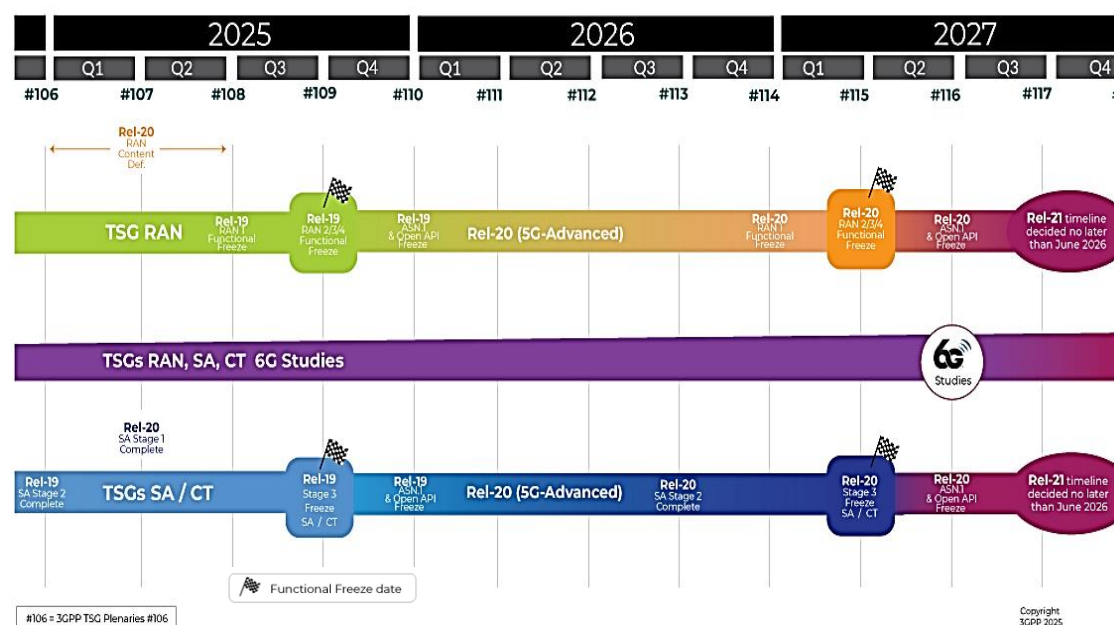
Sinds 2021 heeft O-RAN een snelle groei doorgemaakt en is het O-RAN-ecosysteem en haar marktpositie wezenlijk versterkt. Ondanks deze vooruitgang en het potentieel van flexibiliteit en kostenreductie door de toepassing van O-RAN bestaan nog de nodige technische en operationele uitdagingen zoals de schaalbaarheid, volwassenheid van producten (het bieden van volkomen interoperabiliteit tussen systeemcomponenten) en de levering van adequate technische expertise bij onder meer de integratie in bestaande netwerken. Verder zijn er zorgen over de beveiliging, met discussies over de vraag of openheid het risico vergroot of verkleint.

Op het gebied van standaardisatie speelt in de zin van openheid het verwezenlijken van een goede aansluiting op 3GPP, vooral met het oog op de ontwikkeling van 6G.

6 Update van standaardisatie binnen 3GPP

6.1 Inleiding

3GPP heeft in september 2025 het merendeel van het werk voor Release 19 afgerond⁸⁹, ofwel de tweede release van 5G-Advanced. Ondertussen is 3GPP begonnen met de werkzaamheden rond Release 20. Het plan is om deze maart 2027 inhoudelijk afgerond te hebben⁹⁰. Figuur 7 geeft de huidige 3GPP-tijdplanning aan voor de Releases 19 en 20.



Figuur 7: 3GPP-tijdlijnen voor Release 19 en Release 20 [bron: 3GPP, aangepast]

Zoals weergegeven in Figuur 7 is 3GPP, naast het verbeteren van 5G-Advanced met nieuwe of verbeterde functies, al begonnen met 6G-studies in Release 20. Het eerste 6G-studie-item "6G-gebruiksscenario's (*use cases*) en service requirements" is gestart in september 2024⁹¹ en wordt verwacht eind 2025 te zijn afgerond.

De specificatie van de 6G-standaarden zal naar verwachting starten vanaf Release 21. De planning voor Release 21 moet nog worden bepaald.

Ter voorbereiding op de 6G-studies organiseerde 3GPP in maart 2025 workshops over het 6G Radio Access Network (RAN) en over Service & System Aspects (SA)⁹². Hierin werden 219 presentaties gegeven door 3GPP-leden waaronder leveranciers, operators, de academische

⁸⁹ <https://www.3gpp.org/specifications-technologies/releases/release-19>

⁹⁰ <https://www.3gpp.org/specifications-technologies/releases/release-20>

⁹¹ <https://portal.3gpp.org/desktopmodules/WorkItem/WorkItemDetails.aspx?workItemId=1050110>

⁹² <https://www.3gpp.org/news-events/3gpp-news/6gworkshop-2025>

wereld en marktvertegenwoordigers⁹³. Deze maakten hierin hun visie en prioriteiten voor 3GPP-standaardisatie duidelijk, zo ook de Nederlandse deelnemers TNO en KPN.

6.2 Samenvatting van 6G RAN studies in Release 20

Het gaat hier om een tweetal studies die in respectievelijk de paragrafen 6.2.1 en 6.2.2 zullen worden toegelicht.

6.2.1 Studie naar 6G scenario's/use cases en (RAN) requirements

Sinds Q1 van 2025 buigt de 3GPP RAN-groep zich over de “6G scenario's/use cases en (RAN) requirements”⁹⁴. Naar planning zal deze studie lopen tot Q2 van 2026.

Onderwerpen hierbij zijn bijvoorbeeld 6G-implementatiescenario's, *key performance indicators* (KPI's), architectuur- en migratie-eisen en eisen voor nieuwe en bestaande diensten. Nieuwe diensten die in het 6G-tijdperk worden voorzien, zijn onder andere *immersive communication*, kunstmatige intelligentie ofwel AI, geïntegreerde detectie en communicatie (ISAC: Integrated Sensing and Communication) en niet-terrestrische netwerken (NTN).

De uitkomst van dit onderzoek zal naar verwachting worden gedeeld via de zogenoemde Liaison Statement met de ITU-R WP5D⁹⁵, de ITU-studiegroep die verantwoordelijk is voor de algemene radiosysteemaspecten van internationale mobiele telecommunicatiesystemen (IMT). De uitkomst zal ook worden gebruikt als basis voor de daaropvolgende 6G-studie in 3GPP RAN.

Tot september 2025 is er in de 3GPP RAN-studie een beperkte overeenstemming bereikt over de technische prestatie-eisen voor 6G⁹⁶:

- De gemiddelde spectrale efficiëntie in de downlink zal drie keer zo hoog zijn als die van 5G voor de indoor hotspot- en dichte stedelijke scenario's;
- Voor deze scenario's zal de zogenoemde vijfde percentiele spectrale efficiëntie per gebruiker⁹⁷ in de downlink driemaal zo hoog zijn als die voor 5G;
- Mobiliteitsondersteuning tot 500 km/u;
- De maximale bandbreedte zal 400 MHz bedragen.

De uitkomst van dit onderzoek zal worden vastgelegd in het 3GPP Technisch Rapport TR38.914⁹⁸.

6.2.2 Studie naar 6G Radio

Deze studie staat gepland voor Q3 van 2025 tot en met van Q2 2027 en heeft tot doel om één radiotoegangstechnologie te ontwikkelen die niet door de beperkingen van 5G zal worden gehinderd. Deze ‘6GR’⁹⁹ moet voldoen aan een breed scala aan use cases en eisen

⁹³ <https://www.3gpp.org/about-us/partners>

⁹⁴ <https://www.3gpp.org/news-events/3gpp-news/ran-6g-study1>

⁹⁵ <https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx>

⁹⁶ https://www.3gpp.org/ftp/tsg_ran/TSR_RAN/TSGR_109/Docs/RP-252128.zip

⁹⁷ Dit is een prestatiemaat die de gegevensefficiëntie weergeeft voor de gebruiker met de laagste spectrale efficiëntie, specifiek de 5% van de gebruikers die het laagst presteren.

⁹⁸ <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4392>

⁹⁹ <https://portal.3gpp.org/desktopmodules/WorkItem/WorkItemDetails.aspx?workItemId=1080072>

zoals gedefinieerd tijdens de hierboven genoemde studie naar 6G scenario's/use cases en RAN-eisen.

Het onderzoek naar 6G Radio richt zich op het frequentiebereik tot 52,6 GHz en omvat 'de definitie van:

- Een standalone radionetwerkarchitectuur zodat dus geen rekening hoeft te worden gehouden met de beperkingen van 5G;
- Een fysieke-laagstructuur voor 6GR, inclusief *waveforms* die op OFDM (Orthogonal Frequency Division Multiplexing) zijn gebaseerd;
- Radio-interfaceprotocollen en -procedures voor 6GR;
- Migratie van- en interworking met 5G NR, bijvoorbeeld bij multi-RAT (Radio Access Technology) *handover*;
- Het gebruik van AI voor de 6G-*air interface* en -radionetwerken;
- De ondersteuning van *sensing* in 6GR.

De 3GPP RAN1-groep is vanaf augustus 2025 begonnen met de studie naar de fysieke laag van 6GR (laag 1) en de air interface gevolgd door de RAN2- en RAN3-groepen die vanaf oktober 2025 hun werk zijn begonnen aan de radiotoegangslaag (laag-2) van 6GR en de radionetwerkarchitectuur en -protocollen.

6.3 Samenvatting van 5G-Advanced RAN-functies en -activiteiten in Release 20

Zoals toegelicht in de Monitor najaarseditie van 2024¹⁰⁰, is 5G-Advanced Release 20 bedoeld om de mogelijkheden van 5G Release 19 verder te verbeteren. Meer specifiek betreft dit:

- **Verdere ontwikkeling van MIMO.** Dit onderwerp omvat:
 - De verlaging van de frequentiedichtheid van CSI-RS (Channel State Information Reference Signal) voor een aantal antennes tot 128, zoals in Release 19;
 - De vroegtijdige acquisitie van kanaalstatusinformatie tijdens de statusovergang van de UE (User Equipment) van inactief naar verbonden. Hierdoor kan de UE na de statusovergang direct linkaanpassing uitvoeren (met *closed-up precoding* en een hogere MCS: modulatie- en coderingsschema);
 - Verbetering van de capaciteit en dekking van het uplink Sounding Reference Signal (SRS) in Time-Division Duplex (TDD)-systemen;
- **Studie naar ISAC voor NR.** Op basis van het ISAC-kanaalmodelleringswerk in Release 19 heeft deze studie tot doel om de prestaties van basisstation-gebaseerde monostatische detectie (een enkele gNB met een co-located *sensing*-zender en -ontvanger) voor het UAV-gebruiksscenario te evalueren en daarnaast om de netwerkarchitectuur, procedures en signalering tussen 5G RAN en het core network te bestuderen die nodig zijn voor de ondersteuning van ISAC;
- **Verbetering van de NR-dekking.** Deze is gericht op het verbeteren van de uplink-dekingsprestaties tijdens de eerste toegang, dus wanneer een UE overschakelt van de inactieve modus naar de verbonden modus;
- **Ontwikkeling van NR-NTN.** Niet-terrestrische netwerken ofwel NTN's maken gebruik van satellieten of platforms op grote hoogte zoals vliegtuigen, ballonnen, UAV's en luchtschepen om connectiviteitsdiensten aan te bieden. Ze kunnen terrestrische netwerken aanvullen door dekking te bieden in afgelegen gebieden waar terrestrische

¹⁰⁰ TNO 2024 R12204, December 2024, blz. 9-13

dekking niet beschikbaar is. De ontwikkeling in Release 20 richt zich op de volgende twee functies met betrekking tot de werking van NTN's:

- **GNSS-bestendig functioneren van NR-NTN.** UE's die compatibel zijn met Release 17, 18 en 19 en NTN-toegang ondersteunen, zullen naar verwachting uitgerust zijn met GNSS (Global Navigation Satellite System). Deze UE's zouden voor de uplink tijd- en frequentiecompensatie moeten ondersteunen op basis van hun positie die via GNSS is verkregen. De GNSS-informatie in een UE kan echter tijdelijk minder goed of niet beschikbaar zijn. Deze studie beoordeelt de impact op de initiële toegang en de *connected mode*-procedure voor NR-NTN in dergelijke gevallen;
- **Verbetering van NTN voor Internet of Things (IoT).** NTN voor IoT is gespecificeerd sinds Release 17 maar ondersteunt momenteel geen IMS (IP Multimedia Subsystem)-spraakoproepen via NB-IoT NTN. NB-IoT NTN verwijst naar de Narrowband IoT (NB-IoT)-technologie die gebruikmaakt van NTN, zoals satellieten, om wereldwijde dekking te bieden voor IoT-apparaten met een laag stroomverbruik en lage datasnelheid. Dit werkitem is bedoeld om de verbetering van NB-IoT NTN te specificeren waarbij IMS-spraakoproepen via GSO (Geo-Synchronous Orbit) satellieten zullen worden ondersteund.
- Verdere ontwikkeling van **Ambient IoT**. Ambient IoT streeft ernaar apparaten te voorzien van een sterk verlaagde complexiteit en energieverbruik die vele malen lager liggen dan die van bestaande 3GPP LPWA (Lower Power Wide Area)-technologieën zoals NB-IoT en LTE eMTC (Enhanced Machine Type Communication). Dergelijke apparaten werken ofwel zonder batterij of hebben met alleen een condensator een beperkte energieopslagcapaciteit. Zij worden gevoed via energieopwekking (*energy harvesting*)¹⁰¹. Release 19 specificeert het zogenoemde 'Device 1' (met een stroomverbruik van ongeveer 1 μ W en met transmissie van apparaat naar lezer door middel van *backscattering*) en wel in een zogenaamde 'Topology 1': een richtingsverbinding tussen het Ambient IoT-apparaat en een basisstation-lezer, voor binnenshuis-gebruik. De Release 20-activiteiten omvatten:
 - Een **werkitem** voor de specificatie van oplossingen voor Ambient IoT waarin meerdere combinaties van diverse soorten Ambient IoT-apparaat en topologie-type beschouwd zullen worden. Het gaat dan ook om apparaten die via een UE verbonden zijn met het netwerk; deze IoT-apparaten zijn dus niet afhankelijk van backscattering;
 - Een studie-item over **Ambient IoT voor buitenshuis-gebruik**.
- **Verbeteringen in mobiliteit.** Dit betreft een voortzetting van eerdere releases en is gericht op verdere verbeteringen aan laag 1/2-triggered mobility (LTM). Deze hebben tot doel om het netwerk meer flexibiliteit te bieden om de LTM-configuratie dynamisch te wijzigen. Dit kan plaatsvinden door L2-signalering zonder radio resource control (RRC)-berichten en door het netwerk de mogelijkheid te bieden om secundaire cellen (SCells) dynamisch te activeren;
- **AI/ML voor mobiliteit.** Hier gaat het om de specificatie van:
 - AI/ML-gebaseerde meetvoorspelling voor AI/ML-modellen aan de kant van zowel de UE als het netwerk;
 - Voor een AI-model in een UE, de voorspelling van een meet-event (een vooraf gedefinieerde voorwaarde die een mobiel apparaat activeert om zijn

¹⁰¹ Bestaande mobiele apparaten werken mogelijk niet goed met energieopwekking vanwege hun piekstroomverbruik van meer dan 10 mW

- radiosignaalmetingen aan het netwerk te rapporteren, wat bijvoorbeeld leidt tot een *handover*);
 - Specificatie van signalering en protocollen om levenscyclusbeheer (LCM: Life-cycle Management) mogelijk te maken voor AI/ML-modellen aan UE- en netwerkzijde;
- **Verbeteringen van de AI/ML-interface voor de NR air-interface.** Hier wordt de ondersteuning gespecificeerd voor:
 - Het AI/ML-framework (de signalering en protocollen voor LCM) voor tweezijdige (UE en netwerk) AI/ML-modellen;
 - Verbetering van de feedback van kanaalstatusinformatie (CSI: Channel State Information). In meer detail: dit heeft betrekking op de CSI-ruimtelijke- en frequentiecompressie en de benodigde signalering;
 - De afstemming van de wijze van training en gegevensverzameling van AI/ML-modellen tussen leveranciers onderling;
- **AI/ML voor NG-RAN.** Dit bouwt voort op de werkzaamheden uit Release 18 (AI/ML-use cases voor *load balancing*, energiebesparing en mobiliteitsoptimalisatie) en Release 19 (Op AI/ML-gebaseerde *network slicing* en dekkings- en capaciteitsoptimalisatie). De werkzaamheden voor Release 20 richten zich op AI/ML voor gevallen van mobiliteit zonder UE-invloed zoals intra- en inter-CU¹⁰² LTM;
- **Verbeteringen in de *handover* van 4G TN (Terrestrial Network) naar 5G NTN.** Release 19 bevat oplossingen om in inactieve modus mobiliteit ofwel *handover* tussen 4G LTE TN en 5G NTN mogelijk te maken. In Release 20 ligt de focus op het realiseren van een dergelijke *handover* in de *connected mode*;
- **Ontwikkeling van XR.** Dit werkitem is bedoeld om de nieuwe kenmerken van mobiel AI-verkeer zoals AI-video's, -audio, -afbeeldingen, -tekst en -data en de verschillen met XR-verkeer te identificeren en, indien nodig, verbeteringen te ontwikkelen om efficiënte en effectieve ondersteuning te faciliteren voor mobiele AI-toepassingen en -diensten;
- **Dataverzameling voor zelforganiserende netwerken (SON: Self-Organizing Networks) en Minimization of Drivetest (MDT).** Dit is een voortzetting van eerdere releases, met de focus op optimalisatie van mobiliteitsrobuustheid (MRO: Mobility Robustness Optimization) voor LTM tussen CU's en voor conditionele LTM intra-CU¹⁰³.

¹⁰² CU: Central Unit (van een 5G-basisstation), dit in tegenstelling tot een DU (Distributed Unit) die zich bezighoudt met mobiliteitsprotocollen op lagere lagen, zie TNO 2023 R12053, blz. 22

¹⁰³ In deze context betekent 'conditioneel' dat een UE autonoom kan beslissen wanneer een *handover* moet worden uitgevoerd op basis van de in het netwerk geconfigureerde voorwaarden, in plaats van te wachten op een opdracht na het verzenden van een meetrapport.

7 Tot besluit

Ondanks de groeiende interesse stopt de Monitor Draadloze Technologie na deze editie.

Veel dank aan u, lezer, voor uw belangstelling en vertrouwen in ‘de Monitor’.

Het steeds wisselende team van TNO-experts heeft met veel plezier en inzet de afgelopen decade gewerkt aan de totstandkoming van de nodige edities. Daarbij was de samenwerking met onze externe contacten bij het Ministerie van Economische Zaken altijd heel inspirerend, prettig en waardevol. Ook hiervoor is een woord van dank op zijn plaats.

We wensen u veel wijsheid toe bij het duiden van alles wat op u afkomt aan belangwekkende informatie, zowel over draadloze technologie als daar buiten.

Mede namens het TNO-team,

Ruud Overduin, projectleider vanuit TNO