16 december 2020

Reactie op de internetconsultatie concept-Regeling veiligheid en integriteit telecommunicatie

1. inleiding en samenvatting

Deze reactie betreft 3 aspecten van de concept-Regeling, welke samenhangen en waarvoor onze reactie grotendeels in vragende vorm gesteld wordt:

1. De conceptregeling bevat de door TNO in samenwerking met de huidige netwerkoperators opgestelde aanvullende en technische maatregelen die aanbieders van mobiele telecommunicatie-netwerken dienen te treffen ter beveiliging van hun netwerk. Waarom worden hierbij alleen de netwerken van mobiele netwerkoperators aan nadere regelgeving onderworpen? Zijn of worden vergelijkbare eisen nu of in de toekomst ook aan andere beheerders van publieke en/of kritieke telecommunicatienetwerken of beheerders gesteld van netwerken waar de mobiele operator gebruik van (gaan) maken voor hun dienstverlening? Gaan de maatregelen ook gelden voor netwerkbeheerders van overheids- en utiliteitsnetwerken die mobiele operators mogelijk gaan medegebruiken in de nabije toekomst bij de verdere uitrol van 5G?

2. De regeling richt zich nadrukkelijk op 5G, waarvan de uiteindelijke architectuur en functionaliteit pas in de komende 3GPP releases 16 en 17 vastgesteld zullen gaan worden. In de concept-regeling wordt niet aangegeven wat precies als “kritieke onderdelen” en “kritieke gegevens” wordt beschouwd, maar dit zal pas na vaststelling van de regeling aan betrokken netwerkbeheerders worden medegedeeld. Het begrip “aanpalend” hangt hiermee samen en geldt dezelfde onzekerheid voor. Wat wel gesteld kan worden dat de overall-architectuur van 5G, die al langer geleden is vastgesteld, niet aansluit op de in de regeling beoogde effecten van de voorgestelde beheersmaatregelen.

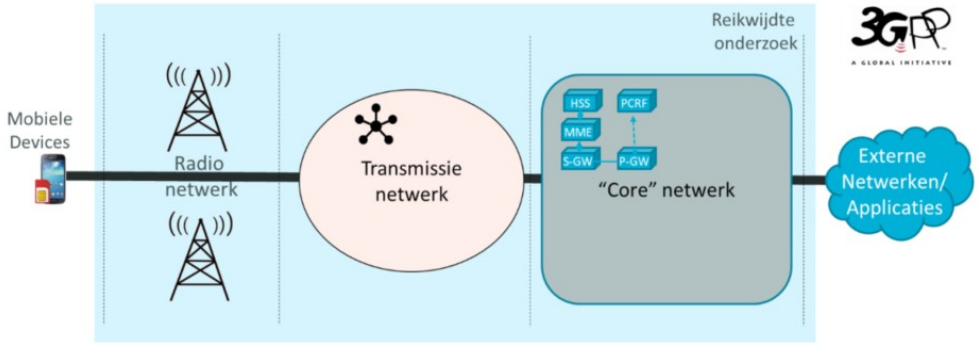
3. De hierboven vermelde onzekerheid over wat precies “kritiek of aanpalend” is en door de beeoogde maatregelen betroffen, geldt wellicht ook voor de (Europees geharmoniseerde 5G) vergunningen in de 700 MHz band voor installaties ter zee. Deze vergunningen worden momenteel via een Verdeling Op Afroep door Agentschap Telecom verdeeld, zie deze publicatie in de Staatscourant, hetgeen kan leiden tot een veiling. Maar wat zijn eventueel de gevolgen van deze consultatie voor de toekomstige bezitters van deze secundaire vergunningen en als de Regeling er niet voor van toepassing wordt verklaard, mogen er dan wel publieke en overheids kritieke telecomdiensten over aangeboden worden?

2. Nadere specificatie 1+2

2.1 Op dit moment worden wereldwijd in toenemende mate 4G radionetwerken gedisaggregeerd en met OpenRAN “gecloudificeerd”, nu nog met name vanwege de energiebesparing, schaalbaarheid en betere beheersmogelijkheden. Maar er zullen straks ook steeds meer 5GC(ore) functies naar de edge verhuizen en hoe kijkt de Taskforce dan aan tegen een neutral host die zowel publieke als private mobiele netwerken bedient? Deze vraag sluit aan op de in de reactie van Nokia vermelde opmerking met als titel “Virtualization increases “critical” footprint” en ook security aspecten zoals versleuteling, authenticatie en authorisaties zullen niet alleen in toenemende mate op

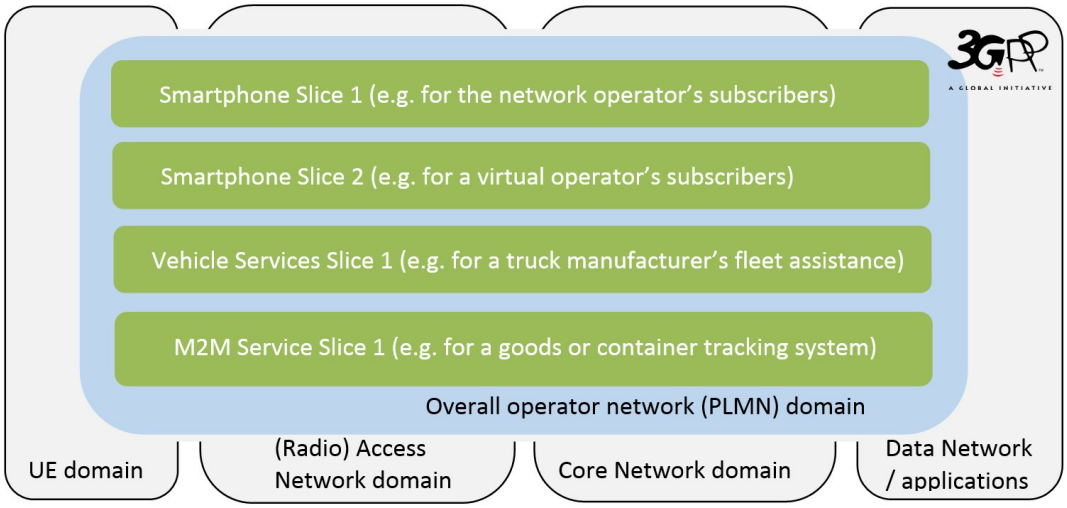
gevirtualiseerde componenten (instanties) afgehandeld worden, maar zeker in 5G netwerken end-to-end worden verspreid (gedisaggregeerd) over de hele communicatieketen.

2.2 Voor de 2 t/m 4G specificaties van het 3GPP consortium wordt de overall technische architectuur meestal weergegeven als een een keten van netwerk-gerelateerde componenten, bestaande uit: eindapparatuur (endpoints) , radioantennenetwerk, transmissienetwerk, core-netwerk en “externe netwerken” (over het algemeen “internet/cloud” en niet-mobiele telecommunicatie-netwerken). Recent werd dit in het Haalbaarheidsonderzoek naar de toekomst van missiekritische breedbandcommunicatie in Nederland door Strict en VKA (Verdonck, Klooster & Associates) in figuur 2 als volgt weergegeven:



Figuur 2. Schematische opbouw mobiel breedbandnetwerk

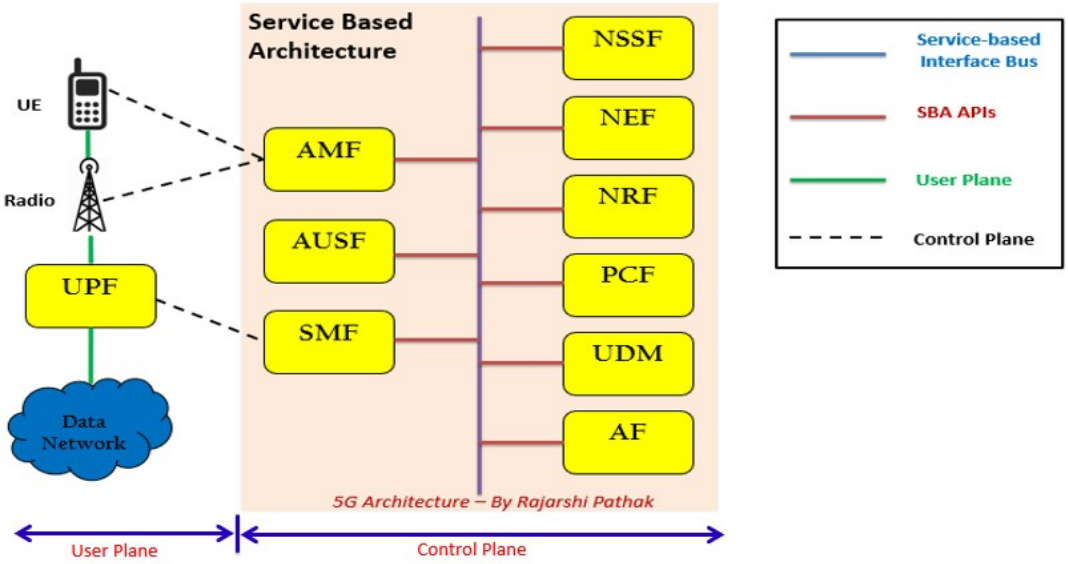
De vertikale stippellijnen geven een compartimentatie aan in netwerkcomponenten die kunnen worden onderscheiden in de communicatieketen, welke zowel beveiligingstechnisch als beheersmatig gescheiden kunnen worden. Bij de publicatie van fase 1 van 5G door 3GGP in 2017 werd echter al duidelijk gemaakt dat vanaf fase2, dus in de releases na 15, met name voor 5G SA uitgegaan wordt van een Service Based Architecture. Hierbij is Network Slicing niet alleen een virtualisatie die daarmee de distributie van de netwerkcomponenten mogelijk maakt, maar een end-to-end service (en security) concept. Onderstaande afbeelding laat duidelijk zien dat slicing de hele keten van UE (User Endpoint) tot (extern) Data Network en applicaties betreft:



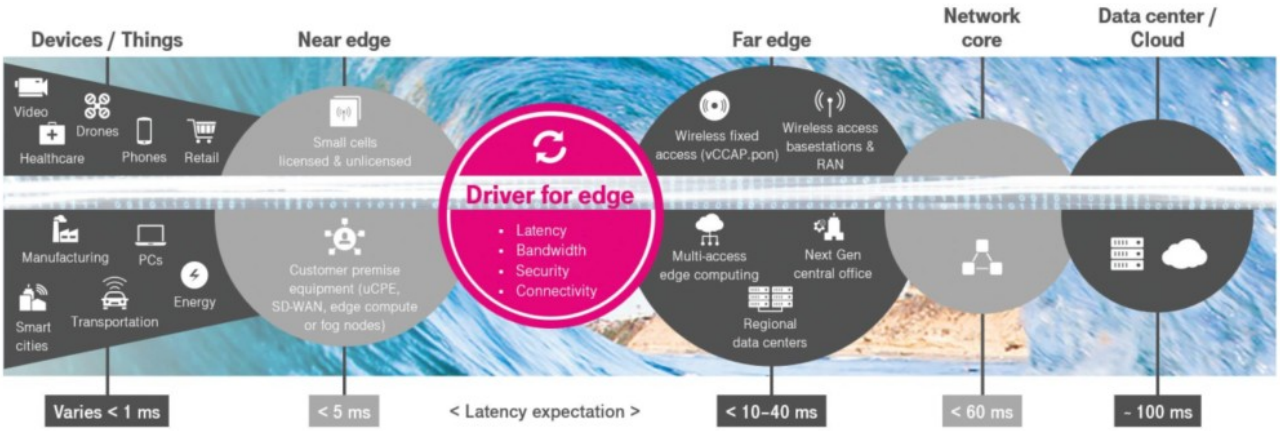
In een dergelijke domeinarchitectuur is het aanscherpen van beheersmaatregelen ten behoeve van veiligheid en integriteit en je daarbij vrijwel uitsluitend richten op het beheer van een “fysiek core netwerk” bij mobiele netwerkoperators niet zinvol.

Figuur 2 in genoemd onderzoeksrapport kan ook gezien worden als exponent van de tradionele (2,3,4G) Reference Based Architecture benadering van mobiele netwerken vanuit de MNO's tot nu toe, waarin met de weergegeven scheiding in netwerkcomponenten het aanbod aan de consumenten met name wordt bepaald door de capaciteit van deze verschillende componenten en de belemmeringen die bij de als verticale stippellijnen weergegeven interfaces hiertussen optreden.

In de 5G-fase-2 wereld met bedrijfs- en missiekritische toepassingen moeten we echter gaan denken en werken vanuit een **Service Based Architecture** en is zowel de UE (User Equipment) als het complete Data Network integraal onderdeel van een 'User Plane'. We spreken hier over de UPF (User Plane Function), waarin de daarin voorziene functionaliteiten als packet routing & forwarding, QoS handling en policy enforcement (en daarmee samenhangende security aspecten) vanuit het Control Plane worden aangestuurd:



Daarnaast zorgen (de voor 5G uiteindelijk onmisbare) ontwikkelingen als 'RAN Cloudification' en 'edge computing' (MEC) ervoor dat we helemaal niet meer over een neutraal "transmissienetwerk" kunnen spreken, maar over een "far edge" en "near edge", waarin naast de gevirtualiseerde RAN-functionaliteiten ook data-opslag en -bewerking plaatsvindt, naast (de minder realtime en energie-zuinige en/of privacy gevoelige) dataverwerking in de traditionele hyperscale datacenters. Deze edge-cloud architectuur voor mobiele netwerken is op onderstaande figuur van T-Systems zichtbaar, waarbij de "edge drivers" bestaan uit "latency, bandwidth, security en connectivity", waarvan de laatste twee in ieder geval zowel voor MCX (missiekritische functionaliteit) als veiligheid en integriteit van essentieel belang zijn:



3. Nadere specificatie 3

In de concepttekst van de Regeling staat dat toekomstige aanbieders van mobiele netwerken die via een veiling over geharmoniseerd radiospectrum gaan beschikken, ook aan de gestelde eisen in deze nu geconsulteerde regeling moeten voldoen. Daarbij wordt een netwerkaanbieder als volgt gedefinieerd: “aanbieder van een openbaar mobiel elektronisch communicatienetwerk die beschikt over vergunningen voor het gebruik van geharmoniseerd radiospectrum als bedoeld in artikel 2, onder 25, van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek van elektronische communicatie (PbEU 2018, L 321) die zijn verleend met toepassing van een veiling, bedoeld in artikel 3.10, eerste lid, aanhef en onderdeel f, van de wet”. Er wordt specifiek gerefereerd aan een veiling als bedoeld in artikel 3.10, eerste lid, onderdeel f. De VOA-procedure valt onder artikel 3.10, eerste lid, onderdeel b. Toch leidt dit tot de volgende vragen:

3.1 Klopt het dat de 700 MHz-vergunningen op zee die via de VOA-procedure worden verdeeld niet onder de reikwijdte van de Regeling veiligheid en integriteit telecommunicatie zullen vallen, ook als de procedure tot verdeling via een veiling leidt?

3.2 Als het nu niet voorzien is in de Regeling dat deze vergunningen hieronder vallen, bestaat er een kans dat de scope als gevolg van de consultatie zodanig verbreed wordt dat vergunningshouders van 700MHz vergunningen op zee (voor het beheer van de netwerken die daarvan gebruik maken) ook (extra) beheersmaatregelen opgelegd krijgen?

3.3 Zo ja, hoe kan een partij die deelneemt aan een eventuele veiling in de VOA-procedure inschatten welke gevolgen dit mogelijk heeft, als de kritieke onderdelen van de mobiele netwerken waarop de beheersmaatregelen zullen toezien, als Departementaal vertrouwelijk zijn aangemerkt en op vertrouwelijke wijze worden gedeeld met de desbetreffende netwerkaanbieders? Kunnen partijen die deelnemen aan de VOA-procedure voorafgaand aan de veiling kennis nemen van deze lijst?