telemach

Agencija za komunikacijska omrežja in storitve RS
Stegne 7
1000 Ljubljana

info.box@akos-rs.si

Ljubljana, 10. 05. 2023

Zadeva: Pripombe in predlogi družbe Telemach Slovenija k osnutku predloga Splošnega akta o dodatnih varnostnih zahtevah in omejitvah

Zveza: **0073-3/2023**

Spoštovani,

sklicujemo se na objavo osnutka Splošnega akta o dodatnih varnostnih zahtevah in omejitvah (»splošni akt«) na spletni strani Agencije za komunikacijska omrežja in storitve RS (»Agencija«) z dne 6. 4. 2023[1] v zvezi s katerim v nadaljevanju v roku, določenem na posvetu z Agencijo dne 08. 05. 2023, podajamo pripombe in predloge, ki se nanašajo zlasti na opredelitev kritičnih elementov, v Prilogi 1 posredujemo predlog sprememb splošnega akta, v Prilogi 2 pa posredujemo podrobna vprašanja. V zvezi z ustavnopravno problematiko predpisa smo se seznanili in se sklicujemo na pravno mnenje o skladnosti nekaterih določb, predvidenih v predlogu Splošnega akta o dodatnih varnostnih zahtevah in omejitvah, z Ustavo Republike Slovenije, ki ga je pripravil izr. prof. dr. Samo Bardutzky pri Inštitutu za primerjalno pravo pri Pravni fakulteti v Ljubljani.

1. Splošno o predlogu

Predlog splošnega akta je že naravnan v smeri, da bo preko zelo striktnih ukrepov, ki jih bodo morali izvajati operaterji, zagotovil zelo visoko stopnjo kibernetske varnosti omrežij. Med te striktne ukrepe lahko štejemo zahtevano certifikacijo vse opreme po 3GPP specifikacijah (NESAS/CSAS), vseobsegajoče načelo ničelnega zaupanja, nadzor nad celotno dobaviteljsko verigo, zelo strikten režim dostopa do omrežja s strani lastnih zaposlenih in zunanjih partnerjev, redno ocenjevanje tveganj in izvajanje mitigacije le teh po zahtevah 5G Toolbox-a. Navedeni ukrepi bodo od operaterjev zahtevali izjemno visok angažma, vendar jih pozdravljamo, saj je zasledujejo legitimen cilj zagotovitve visoke varnosti omrežij.

Predlagani splošni akt med seznam kritičnih sredstev, v nasprotju z Nacionalno oceno tveganja kibernetske varnosti 5G v Republiki Sloveniji[2], ki je bila posredovana Evropski Komisiji in Agenciji

[1] https://www.akos-rs.si/javna-posvetovanja-in-razpisi/novica/agencija-objavlja-predlog-splosnega-akta-o-dodatnih-varnostnih-zahtevah-in-omejitvah
[2] Nacionalna ocena tveganja kibernetske varnosti 5G v Republiki Sloveniji je bila pripravljena na podlagi prispevkov

Evropske unije za kibernetsko varnost ter relevantnimi smernicami evropskih organizacij, ki jih navajamo v nadaljevanju, uvršča tudi radijsko dostopovno omrežje (»RAN«), ter z RAN povezane upravljavske sisteme z nadzorom delovanja in upravljanja omrežja, ki vključujejo RAN/O-RAN in jih obravnavamo skupaj kot radijsko dostopovno omrežje. Uvrstitev radijskega dostopovnega omrežja je izvedena na tehnično in nomo-tehnično nenavaden način, z opredelitvijo:

»Bazne postaje, ki podpirajo tehnologijo 5G ali višje, katerih sevalno območje sega na območje objektov kritične infrastrukture.«

Predlagatelj se je pri pripravi splošnega akta moral zavedati,

- prvič, da da »objekti kritične infrastrukture« sploh niso javno objavljeni, kar pomeni, da sploh ni mogoče vedeti, katere bazne postaje so torej kritične in
- drugič, da je kritična infrastruktura v Zakonu o kritični infrastrukturi (s katerim se edino državljan lahko seznani), opisana neverjetno široko, kot *»sektor energetike, sektor prometa, sektor prehrane, sektor preskrbe s pitno vodo, sektor zdravstva, sektor financ, sektor varovanja okolja ter sektor informacijsko-komunikacijskih omrežij in sistemov«,* kar praktično lahko predstavlja vsak elektro števec, cesto, pipo, bolnišnico, bankomat, čistilno napravo ali modem.

Ni se mogoče izogniti vtisu, da se je predlagatelj splošnega akta želel s tako opredelitvijo izogniti lastnim ugotovitvam v Nacionalni oceni tveganja kibernetske varnosti 5G v Republiki Sloveniji, ki radijskega omrežja ne opredeljuje kot kritičnega in se hkrati izogniti morebitni odškodninski odgovornosti za škodo oz. posledice omejevanja konkurence z oblastnimi akti in ravnanji, ki bi jo z zlorabo opredelitve zadal prizadetim podjetjem, hkrati pa dosegel svoj cilj – tj. arbitrarno določitev celotnega ali kateregakoli področja v Sloveniji kot prepovedanega za določeno opremo.

V zvezi s tem je potrebno izpostaviti, da je zgolj z uporabo naprednih razlagalnih pravil mogoče izluščiti naslovnike oz. zavezance za izpolnjevanje dodatnih varnostnih zahtev. Prvi odstavek 116. člena ZEKom-2[3] namreč za zavezance določa operaterje »*mobilnih komunikacijskih omrežij, ki zagotavljajo ta* ***omrežja*** *upravljavcem kritične infrastrukture«*. V skladu z definicijami iz 3. člena ZEKom-2 in običajno

štirih telekomunikacijskih operaterjev (Telekom Slovenije, T-2, Telemach, A1) in nacionalnih organov, pristojnih za nacionalno varnost (Ministrstvo za notranje zadeve, Policija, Ministrstvo za obrambo, Slovenska obveščevalno-varnostna agencija, Urad Vlade RS za varovanje tajnih podatkov), ki jih skupaj usklajujeta Agencija za komunikacijska omrežja in storitve in Ministrstvo za javno upravo.

[3] *(1)* ***Operaterji mobilnih komunikacijskih omrežij, ki zagotavljajo ta omrežja upravljavcem kritične infrastrukture*** *z drugih področij urejanja kritične infrastrukture, določenim v skladu z zakonom, ki ureja področje kritične infrastrukture (v nadaljnjem besedilu: upravljavci kritične infrastrukture), izvajalcem bistvenih storitev, določenih v skladu z zakonom, ki ureja informacijsko varnost (v nadaljnjem besedilu: izvajalci bistvenih storitev), organom državne uprave, določenim v skladu z zakonom, ki ureja informacijsko varnost (v nadaljnjem besedilu: organi državne uprave) oziroma nosilcem ključnih delov sistema varnosti države, morajo poleg zahtev iz prejšnjega člena upoštevati dodatne varnostne zahteve in omejitve.*

uporabo pojma »komunikacijsko omrežje« (med katere spadajo elektronska[4], javna[5], odprta[6]) **se (elektronsko) komunikacijsko omrežje**, »*Elektronsko komunikacijsko omrežje so sistemi prenosa,[…] ki omogočajo prenos signalov po […] ne glede na vrsto prenesenih informacij.",* **razlikuje od elektronskih komunikacijskih storitev**, ki so opredeljene posebej v 6. točki 1. odst. 3. člena ZEKom-2, z opredelitvijo: *»Elektronska komunikacijska storitev je storitev, ki se navadno izvaja za plačilo prek elektronskih komunikacijskih omrežij […]«,* navsezadnje pa je razlikovanje vzpostavljeno že v prvem stavku prve povedi prvega člena[7] ZEKom-2, kjer je namen zakona najprej urejanje omrežij in nato urejanje storitev.

Zakonodajalec je v nadaljevanju v 4. odst. 116. člena ZEKom-2 med naslovnike obveznosti izpolnjevanja dodatnih varnostnih zahtev vključi ponudnike omrežij in storitev, ki niso javna, s čimer pojasni dodatno področje urejanja. Ob upoštevanju navedenih opredelitev je potrebno iz zakonske norme izluščiti vrsto omrežja iz 1. odstavka, ki ga operaterji mobilnih komunikacijskih omrežij nudijo upravljalcem kritične infrastrukture in ostalim subjektom 1. odstavka, saj tako omrežje ne more biti zasebno (ker je navedeno ločeno v 4. odst.), tako da ostane zgolj javno komunikacijsko omrežje (in ne storitve), nudeno upravljalcem kritične infrastrukture, izvajalcem bistvenih storitev in organom državne uprave. Edina oblika javnega komunikacijskega omrežja, ki se na tak način lahko nudi, je zgolj komunikacijsko omrežje, ki bi ga navedene tri kategorije uporabnikov uporabljale kot MVNO, torej kjer s pravnim poslom uporabnik pridobi pravico do uporabe omrežja v določenem obsegu, pri čemer bi v takem primeru celo šlo za self-supply, torej MVNO zagotovljen sam sebi. Striktno gledano je zakonsko pooblastilo Agenciji zgolj urejati dodatne varnostne zahteve za omrežja, ki jih upravičenci najamejo za svoje potrebe in hkrati niso zasebna omrežja ter za omrežja, ki jih upravičenci najamejo za svoje potrebe in so zasebna omrežja. 1. odstavek 116. člena torej ne zajema elektronskih komunikacijskih storitev, ki bi jih operater upravičencem iz. 1. člena nudil kot končnim uporabnikom. Ne glede na to, da upravičencev iz 1. člena, ki bi gospodarno lahko upravljali MVNO ni, njihova uvedba pa bi operaterja (v praktičnem smislu, v izogib igranju igre Minolovec) da bi se izognil pokrivanju prepovedane infrastrukture, izpostavila obveznosti zagotavljanja dodatnih varnostnih zahtev za celotno območje Republike Slovenije. Agencijo tako pozivamo na previdnost in premišljenost pri določanju kritičnih elementov.

2. Opredelitev kritičnih elementov v relevantnih virih

1. Splošno priznano tehnično dejstvo je, da se različni deli omrežja 5G razlikujejo po občutljivosti in ranljivosti. V skladu z *usklajeno oceno tveganja EU za kibernetsko varnost omrežij 5G*[8] in *Zbirko orodij*

[4] 8. tč. 1. odst. 3. člena ZEKom-2, *Elektronsko komunikacijsko omrežje so sistemi prenosa, ne glede na to, ali temeljijo na stalni infrastrukturi ali zmogljivosti s centralnim upravljanjem, in, kjer je primerno, komutacijska ali usmerjevalna oprema ter drugi viri, vključno z neaktivnimi omrežnimi elementi, ki omogočajo prenos signalov po žicah, z radijskimi valovi, optičnimi ali drugimi elektromagnetnimi sredstvi, vključno s satelitskimi omrežji, fiksnimi (vodovno in paketno komutiranimi, vključno z internetom) in mobilnimi omrežji, električnimi kabelskimi sistemi, če se uporabljajo za prenos signalov, z omrežji, ki se uporabljajo za radijsko in televizijsko radiodifuzijo, ter z omrežji kabelske televizije ne glede na vrsto prenesenih informacij.*

[5] 23. tč. 1. odst. 3. člena ZEKom-2

[6] 48. tč. 1. odst. 3. člena ZEKom-2

[7] *Ta zakon ureja pogoje za zagotavljanje elektronskih komunikacijskih omrežij in izvajanje elektronskih komunikacijskih storitev […]*

[8] Usklajena ocena tveganja EU za kibernetsko varnost v omrežjih 5G: P16-P18; https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 s

EU za kibernetsko varnost omrežij 5G za ukrepe za zmanjšanje tveganja[9] ("Zbirka orodij EU"), ki so jo pripravile skupine za sodelovanje NIS[10] , ter *dodatkom 5G - k Smernicam o varnostnih ukrepih v okviru EECC*[11] , ki ga je pripravila ENISA (Agencija Evropske unije za kibernetsko varnost), je treba RAN obravnavati kot "HIGH" v primerjavi s CORE in NFV, ki se obravnava kot "CRITICAL". Varnostne zahteve, ki jih vsebuje Seznam kritičnih sredstev splošnega akta, so tako v nasprotju z viri, ki jih citira navedeni akt in Splošni akt o varnosti omrežij, storitev in podatkov.

2. V skladu s standardi ETSI/3GPP, tj. TR 121 915 - V.15.0.0, jasno razvršča omrežna sredstva z različno stopnjo tveganja. Kot kritične so opredeljene samo funkcije jedrnega omrežja ter upravljanje in orkestracija omrežja NFV.

-Network assets

CATEGORIES OF ELEMENTS AND FUNCTIONS		EXAMPLES OF KEY ELEMENTS
Core network functions	CRITICAL	User Equipment Authentication, roaming and Session Management Functions
		User Equipment data transport functions
		Access policy management
		Registration and authorization of network services
		Storage of end-user and network data
		Link with third-party mobile networks
		Exposure of core network functions to external applications
		Attribution of end-user devices to network slices
NFV management and network orchestration (MANO)	CRITICAL	
Management systems and supporting services (other than MANO)	MODERATE/HIGH	Security management systems
		Billing and other support systems such as network performance
Radio Access network	HIGH	Base stations

Radijske bazne postaje (spodaj predstavljene kot DU/CU) veljajo za manj občutljiv element arhitekture omrežja, ki jo prikazuje 3GPP. Koncept je prikazan v diagramu, kot je prikazan na skici - omrežne funkcije, kot sta UDM ali ARPF, zahtevajo najvišjo raven zaupanja, radijske bazne postaje (predstavljene kot DU/CU) pa veljajo za veliko manj občutljiv element arhitekture omrežja. Opredelitev

[9] Zbirka orodij EU: EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures P39-P40, dostopno na https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[10] Skupina za sodelovanje na področju omrežnih in informacijskih sistemov je bila ustanovljena z direktivo o varnosti omrežij in informacijskih sistemov, da bi dosegla *visoko skupno raven varnosti omrežnih in informacijskih sistemov v EU*. Skupino za sodelovanje NIS sestavljajo predstavniki držav članic EU, Evropske komisije in Agencije EU za kibernetsko varnost (ENISA).

[11] Dodatek 5G k Smernici o varnostnih ukrepih v okviru EECC: P8, dostopno na spletni strani https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc.

RAN in transportnih funkcij je torej v nasprotju z ETSI in 3GPP standardi. Plastično povedano, RAN ni izpostavljen proti javnemu Internetu in s tem potencialnim zlorabam s strani tretje strani ali celo dobavitelja, temveč je povezan le preko 3GPP standardiziranih vmesnikov do jedra, jedro pa preko ognjenih pregrad do Interneta. S striktnim režimom upravljanja z dostopi (vključno dostopi dobavitelja) do omrežja, ima operater poln nadzor nad preprečevanjem zlorab s katerekoli strani.

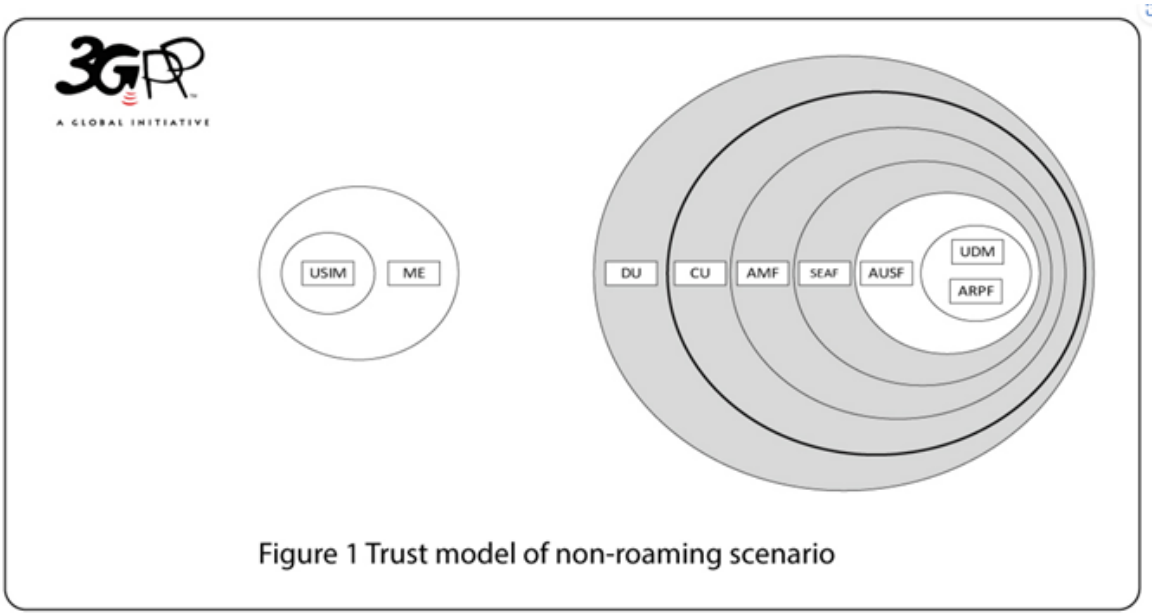

Figure 1 Trust model of non-roaming scenario

3. Tehnično pojasnilo o občutljivosti RAN in funkcij transporta in prenosa

1. Radijsko dostopovno omrežje (RAN): RAN ne nadzoruje dostopa do omrežja in prometa na bistven način in velja za manj občutljiv element arhitekture omrežja. Sedanji in prihodnji razvoj 5G RAN v zadnjem letu verjetno ne bo spremenil operativnega modela RAN. Profil tveganja, opredeljen v orodju 5G Toolbox za RAN, ki ni kritičen, še vedno velja. Trenutno je po vsem svetu v komercialni uporabi več kot tri milijone baznih postaj 5G pod okriljem 3GPP in za bazne postaje niso bile ugotovljene ranljivosti, ki bi utemeljevale oceno baznih postaj kot »kritičnih sredstev«.

2. Funkcije transporta in prenosa: V skladu s tehničnimi ocenami Evropske komisije *"vse jedrne funkcije omrežja 5G na splošno veljajo za kritične",* medtem ko je omrežje RAN *"ocenjeno kot razmeroma visoko občutljivo",* transportno omrežje pa je "*ocenjeno kot zmerno do visoko občutljivo"*. Pri transportnih in prenosnih funkcijah gre le za posredovanje prometnih podatkov in ne morejo ničesar storiti za nadzor ali vplivanje na promet v velikem obsegu, zato tveganje ni tako visoko kot pri jedru ali celo RAN.

4. Praksa v drugih državah EU

Izrecna opredelitev RAN kot kritične ni običajna praksa v EU. Npr. Avstrija ne uvaja opredelitve v zvezi

s kritičnimi omrežnimi komponentami[12], nemški pristojni organ, vključno z regulativnim organom za kibernetsko varnost BSI **(**Das Bundesamt für Sicherheit in der Informationstechnik, "BSI") in regulativnim organom za telekomunikacije BNetzA (Bundesnetzagentur, "BNetzA"), kritičnih komponent ne opredeljujeta po lastni presoji. Operaterji morajo na podlagi seznama, ki ga zagotovita BSI in BNetzA, določiti, katera komponenta se šteje za "kritično komponento". Finski telekomunikacijski organ Traficom v skladu z EU 5G toolbox definicijo opredeljuje kot "ključne funkcije in ukrepe omrežja, ki se uporabljajo za nadzor in upravljanje dostopa do omrežja in omrežnega prometa na *pomemben* način" (poudarek dodan) s posebnim seznamom, ki *ne vključuje radijskega dostopovnega omrežja 5G (RAN), prenosa in prenosnega omrežja, storitev in omrežnih elementov za povezovanje opreme omrežij 5G ter za tajni nadzor elektronskega komunikacijskega omrežja*.[13] Madžarska ne uvaja opredelitve kritičnih omrežnih komponent ali kakršnih koli omejitev.

5. Podrobneje o pravni problematiki »kritične infrastrukture«[14]

Pojem *objekta kritične infrastrukture* ni definiran. Zakon o kritični infrastrukturi sicer definira sektorje kritične infrastrukture,[15] a iz te definicije v konkretnem primeru ni mogoče presoditi, ali je nek objekt del kritične infrastrukture ali ne. Enako velja za omembo objektov kritične infrastrukture v prvem odstavku 128. člena Zakona o katastru nepremičnin,[16] Zakon o obrambi pa določa po eni strani pravila v zvezi z upoštevanjem obrambnih potreb pri infrastrukturnih objektih (28. člen) in po drugi strani definira obrambne objekte (29. člen),[17] kar so nedvomno pravne norme z ožjim poljem uporabe. Iz tega sledi, da je definicija baznih postaj, ki se štejejo za kritična sredstva, takšna, da iz nje z uporabo uveljavljenih metod pravne razlage ni mogoče zanesljivo ugotoviti, kaj sploh so tiste točke v prostoru, na katere ne sme segati sevalno območje bazne postaje, da bi se ta štela za kritično sredstvo. To naslovnikom pravne norme povsem onemogoča, da bi svoja ravnanja prilagodili predpisom in se izognili negativnim posledicam potencialne kršitve pravne norme.

6. Problematika določanja vsebine pravnih poslov, ki jih bodo operaterji sklepali z dobavitelji

7. točka prvega odstavka 3. člena predloga splošnega akta določa usmeritve, ki naj bi jim sledil operater pri sklepanju dobaviteljskih pogodb, hkrati pa peti odstavek 6. člena predloga splošnega akta nalaga izogibanje dolgoročnim pogodbam z dobavitelji. Obe določbi presegata zakonsko pooblastilo iz petega odstavka Zakona o elektronskih komunikacijah, saj jasno presega pooblastilo za določitev "drugih zlasti tehničnih usmeritev", kot se glasi zakonsko pooblastilo, saj gre za prepoved, ki ne more biti prepuščena podzakonskemu urejanju, in je tako v nasprotju z določili 87. člena Ustave RS. *Cybersecurity of 5G*

[12] V skladu z avstrijskim zveznim zakonom o telekomunikacijah (Zakon o telekomunikacijah - TKG 2021) ni opredelitve kritičnih omrežnih komponent. Dostopno na spletni strani https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2021_1_190/ERV_2021_1_190.pdf

[13] Uredba o kritičnih delih komunikacijskega omrežja, TRAFICOM/161584/03.04.05.00/2020, povezava: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Regulation_on_critical_parts_of_a_communications_network.pdf

[14] Poglavje citirano iz izr. prof. dr. Samo Bardutzky, Pravno mnenje o skladnosti nekaterih določb, predvidenih v predlogu Splošnega akta o dodatnih varnostnih zahtevah in omejitvah, z Ustavo Republike Slovenije, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, April 2023

[15] 13. točka 3. člena Zakona o kritični infrastrukturi (Uradni list RS, št. 75/17 in 189/21 - ZDU-IM)

[16] Uradni list RS, št. 54/21

[17] Zakon o obrambi (Uradni list RS, št. 103/04 - uradno prečiščeno besedilo, 95/15 in 139 ni/20).

Networks - EU Toolbox of risk mitigating measures, tveganja dopušča zmanjšati tudi z manj invazivnimi ukrepi, kar pomeni, da taka določila niso nujna za doseganje zakonskih ciljev in so tako nesorazmerna.

7. Sklepno

Iz povedanega zaključujemo, da je vključitev RAN skupaj z nadzorom delovanja in upravljanja omrežja (RAN/O-RAN) in funkcij transporta in prenosa v seznam kritičnih sredstev v nasprotju z relevantnimi strokovnimi viri in ga hkrati v praksi sploh ni mogoče izvajati razen s celotno (izredno finančno in organizacijsko zahtevno) menjavo omrežja v primeru opredelitve določene opreme radijskega dostopovnega omrežja in storitev podpore tretje ravni kot prepovedane. S tako opredelitvijo bi operaterju nastala najprej neposredna škoda, hkrati pa še težko popravljiva posredna škoda na trgu, ki bi bila težko nadomestljiva ne le za operaterja, temveč tudi za končne uporabnike, saj že pred leti opravljene študije[18] v zvezi z zmanjšanjem koristi za končne uporabnike v primeru oviranja enega izmed operaterjev le-to ocenjujejo na pribl. 300 milijonov EUR v obdobju 10 let.

V izogib navedenemu Agencijo pozivamo, da splošni akt prilagodi tako da:

- da se omeji na prilogo in odstrani opisno opredelitev iz 2. točke prvega odstavka 2. člena, ter
- Seznam kritičnih sredstev v prilogi splošnega akta prilagodi tako, v tabeli zbriše kategoriji Radijsko dostopno omrežje in Transport in prenosne funkcije ter funkcionalnost Nadzor delovanja in upravljanja omrežja (RAN/O-RAN) v kategoriji Upravljavski sistemi in drugi podporni sistemi kot prikažemo v Prilogi 1.

S spoštovanjem,

Tony Štupar
Oddelek za pravne zadeve in regulativo

telemach
Telemach d.o.o. 12

[18] doc.dr. Aljoša Feldin, Ocena škode povzročene trgu storitev mobilnih komunikacij zaradi izrivanja tretjega največjega konkurenta, Ljubljana 2016

telemach

Priloga 1 – Predlagano brisanje kategorij in funkcionalnosti

Kategorija	Funkcionalnost
Upravljanje z naročniki in šifrirni mehanizmi	- Upravljanje s sejami (govor in podatki), - Avtentikacija uporabnikov in opreme z omrežjem, - Upravljanje in hramba ključev za avtorizacijo naročnikov in omrežnih komponent (UICC/eUICC, digitalna potrdila/HSM), - Funkcije za varno avtentikacijo, varovanje celovitosti komunikacije (šifriranje) in shranjevanje uporabniških ključev, komponent omrežja in upravljanja, - Upravljanje dostopnih pravic.
Vmesniki za medomrežno povezovanje	- Funkcije gostovanja (signalizacija prometa, izmenjava CDR zapisov, sistemi za zaznavanje zlorab), - Funkcije in poizvedbe v povezavi s prenosljivostjo številk - Vmesniki in povezave do drugih omrežij in ponudnikov vsebin
Upravljane omrežne storitve	- Registracija in avtorizacija omrežnih storitev, - Hramba in obdelava komunikacijskih, lokacijskih in prometnih podatkov, - Izpostavljenost omrežja in omrežnih funkcij zunanjim aplikacijam in storitvam.
Upravljanje virtualiziranih omrežnih funkcij (NFV) in omrežna orkestracija (MANO), vključno z virtualizacijsko infrastrukturo	- Upravljavske funkcije orkestracije in konfiguracije NFV ne glede na tip implementacije (VM, kontejner, mikro- storitve) - Virtualizacijske funkcije za izvedbo in uporabo NFV, - Funkcije izbire in uporabe omrežne rezine (NSSF),
~~Radijsko dostopovno omrežje~~	~~- Bazne postaje, ki podpirajo tehnologijo 5G ali višje, katerih sevalno območje sega na območje objektov kritične infrastrukture.~~
Upravljavski sistemi in drugi podporni sistemi	~~- Nadzor delovanja in upravljanja omrežja, vključno z dostopovnim delom (RAN/O-RAN),~~ - Nameščanje in administracija virtualiziranih omrežij in podomrežij, - Sistemi zaznavanja varnostnih dogodkov, anomalij, groženj in njihovo upravljanje (varnostne funkcije vključno s SIEM/SOAR)
~~Transport in prenosne funkcije~~	~~- Transportne funkcije, ki omogočajo prenos in usmerjanje občutljivega govora in podatkov (usmerjanje, SMSC, IMS).~~
Zakonito prestrezanje	- Funkcije dostopa do vsebine komunikacije in meta podatkov uporabnikov s strani pristojnega organa

telemach

Priloga 2: Vprašanja Agenciji za komunikacijska omrežja in storitve v okviru javne razprave

1. Zakaj definicija kritičnih sredstev (oz. elementov in funkcij omrežja) iz predloga splošnega akta odstopa od predhodnih stališč Republike Slovenije zavzetih v razmerju do EU (konkretno dokument National 5G Cybersecurity Risk Assessment of the Republic of Slovenia iz 2019, katerega pripravo je koordiniral ravno AKOS ob sodelovanju številnih deležnikov in je tvoril podlago za usklajeno oceno tveganj na nivoju EU, ki jasno razmejuje med kritičnimi deli omrežja (jedrni del omrežja (core) skupaj z upravljanjem virtualiziranih omrežnih funkcij (NFV) in omrežno orkestracijo (MANO) in nekritičnimi deli omrežja (kamor se prišteva radijsko dostopovno omrežje ter transport in prenosne funkcije))?

2. Zakaj definicija kritičnih sredstev iz predloga splošnega akta odstopa od smernic EU, to je Nabora orodij EU za kibernetsko varnost (EU toolbox on 5G Cybersecurity, stran 39 in 40), Usklajene ocene tveganj za kibernetsko varnost omrežij 5G (EU Coordinated risk assessment of the cybersecurity of 5G networks, glejte stran 16,17) in tudi mednarodnih standardov, npr. 3GPP (vsem navedenim je skupno, da jasno razmejujejo med kritičnimi deli omrežja (jedrni del omrežja (core) skupaj z upravljanjem virtualiziranih omrežnih funkcij (NFV) in omrežno orkestracijo (MANO)) in nekritičnimi (kamor se prišteva radijsko dostopovno omrežje ter transport in prenosne funkcije ter upravljavski sistemi in drugi podporni sistemi)?

3. Zakaj predlagana ureditev odstopa od dobrih praks iz drugih držav EU, npr. Nemčije, Avstrije, Madžarske, Finske, itd.?

4. Ali je AKOS naredil poglobljeno presojo posledic predloga splošnega akta vključno z vplivom na konkurenco, tako na nivoju operaterjev kot tudi dobaviteljev opreme (vključno z rizikom splošnih podražitev opreme tudi za operaterje, ki morebiti opreme zadevnega dobavitelja, za opremo katerega bi bila izdana odločba vlade po 117. členu ZEKom-2 sploh ne uporabljajo), stroški za operaterje in v končni posledici za potrošnike, pa tudi v kontekstu ciljev ¬Republike Slovenije glede razvoja omrežij in ambicioznih načrtov Strategije razvoja informacijske družbe Republike Slovenije do leta 2030, Krovne strategije razvoja informacijske družbe do leta 2030 in Načrta razvoja gigabitne infrastrukture do leta 2030, vse v kontekstu prepovedi opreme v povezavi s kriteriji, ki so potencialno diskriminatorni in lahko nimajo nobene vzročne zveze z varnostjo omrežij?

5. Ali je AKOS naredil analizo potencialne škode (tako za dobavitelje opreme, kot tudi za operaterje in končne uporabnike vključno s potrošniki) in morebitne odškodninske odgovornosti Republike Slovenije, če bi se ukrepi izkazali za neustavne, kot kaže mnenje ustavno-pravnega strokovnjaka, prof. dr. Samo Bardutzky-ja, predstojnika katedre za ustavno pravo Pravne fakultete Univerze v Ljubljani, ki ga je prejel AKOS in so ga v vednost prejeli nekateri deležniki (npr. v primeru intervencije Ustavnega sodišča, ki bi lahko poseglo v splošni akt) ali sicer protipravne ali v nasprotju s pravom EU ali mednarodnim pravom? Vse ob upoštevanju, da je vzdrževanje, obnavljanje in nadgrajevanje omrežja kontinuiran proces in da bi navkljub prehodnemu obdobju 7 let iz ZEKom-2 posledice morebitne izdane odločbe v povezavi s splošnim aktom začele nastopati takoj.

telemach

6. Ali je AKOS preučil dolžnost predhodne notifikacije splošnega akta po TRIS mehanizmu (po SMT Direktivi, t.j. Direktiva (EU) 2015/1535) oziroma členu 2.9.2 Sporazuma o tehničnih ovirah v trgovini (TBT) (AKOS je na primer po TRIS mehanizmu objavil Splošni akt o načrtu uporabe radijskih frekvenc, vprašanje pa je, zakaj ni enako ravnal glede relevantnega Splošnega akta)?

7. Ali je bila narejena analiza skladnosti oz. neskladnosti predlaganega splošnega akta z vidika prava varstva konkurence?

8. Ali je bila narejena analiza potencialne kršitve Sporazuma o tehničnih ovirah v trgovini (TBT) oziroma prava svetovne trgovinske organizacije (WTO)?