telemach

Agencija za komunikacijska omrežja in storitve RS
Stegne 7
1000 Ljubljana

info.box@akos-rs.si

Ljubljana, 18.9.2023

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

Zveza: Sklicna številka: **0073-3/2023**

Spoštovani,

sklicujemo se na objavo novega osnutka Splošnega akta o dodatnih varnostnih zahtevah in omejitvah (»splošni akt«) na spletni strani Agencije za komunikacijska omrežja in storitve RS (»Agencija«) z dne 7. 8. 2023[1] v zvezi s katerim v nadaljevanju v roku podajamo pripombe in predloge. V zvezi s tem se smiselno sklicujemo na pripombe in predloge, ki smo jih že podali k prvi različici, kjer smo obširno tehnično prikazali, da noben izmed mednarodnih standardov ne šteje radijskega omrežja kot kritičnega in zakaj. Hkrati se je družba Telemach Slovenija seznanila in se v celoti sklicuje tudi na pravno mnenje Inštituta za primerjalno pravo pri Pravni fakulteti Univerze v Ljubljani.[2] Predlog spremembe Splošnega akta prilagamo v Prilogi 1, izrecna vprašanja Agenciji pa v Prilogi 2.

POVZETEK

1. Uvodoma pojasnimo, da ne obstajajo spremenjene okoliščine in dejstva, ki bi podpirala objavo novega predloga akta na način, kot je to storila Agencija.
2. V drugi točki pojasnimo, da vse domače in tuje strokovne podlage, ki jih v zvezi z vključitvijo RAN med kritične elemente navaja Agencija, podpirajo ravno nasprotne zaključke, torej, da RAN ne spada me kritične elemente.
3. V tretji točki opišemo metodologijo za ocenjevanje tveganj, ki bi jo bilo potrebno izvesti za kakršenkoli zaključek, kateri elementi so lahko opredeljeni kot kritični.
4. V četrti točki opišemo razumne pristope, ki so uporabljeni npr. v Avstriji, Nemčiji, na Finskem in na Madžarskem.

[1] https://www.akos-rs.si/javna-posvetovanja-in-razpisi/novica/agencija-objavlja-nov-predlog-splosnega-akta-o-dodatnih-varnostnih-zahtevah-in-omejitvah
[2] Pravno mnenje o skladnosti nekaterih določb, predvidenih v predlogu Splošnega akta o dodatnih varnostnih zahtevah in omejitvah, z Ustavo Republike Slovenije, izr. prof. dr. Samo Bardutzky, univ. dipl. pravnik, strokovni sodelavec na področju ustavnega prava, Ljubljana, 11. 9. 2023

5. V peti točki se dotaknemo tudi preseganja zakonskega mandata Agencije, kjer Agencija želi predpisati pogodbeno vsebino z dobavitelji nad pooblastilom, ki ga daje ZEKom-2.
6. V šesti točki pojasnimo obširne in resne ekonomske posledice za nacionalno gospodarstvo in družbo v primeru sprejema splošnega akta v trenutni obliki.

1. Ratio in ratio legis novega osnutka

Navedeni nov osnutek naj bi bil (brez opredelitve do že podanih pripomb) po navedbah Agencije potreben zaradi več pomembnih dogodkov, ki so se zgodili na nacionalnem in na evropskem nivoju in ki vplivajo na vsebino in zahteve predmetnega splošnega akta. Agencija naj bi, po svojih lastnih navedbah, *pripravila nov predlog splošnega akta v luči navedenih sprememb na evropski in nacionalni ravni in po posvetovanju in na podlagi dejstev in ugotovitev, ki izhajajo iz priporočila Urada Vlade za informacijsko varnost (URSIV)*. Niti navedenih dogodkov, niti dejstev in ugotovitev, ki naj bi bili podlaga za tako odločitev, niti kakšno odločitev je Agencija pravzaprav sprejela, Agencija sicer ne razkrije in se do njih ni mogoče opredeliti, kar operaterje in druge deležnike dejansko sili v špekuliranje. Tak pristop za sprejemanje podzakonskega akta na podlagi zakonskega pooblastila je v nasprotju z načelom legalitete, ki je tesno povezano z načeli demokratičnosti (1. člen Ustave RS), pravne države (2. člen Ustave RS) in delitve oblasti (3. člen Ustave RS), iz katerih izhajata obveznosti delovanja izvršilne veje oblasti na vsebinski podlagi in v okviru zakona in prepoved spreminjanja ali originarnega (izvirnega) urejanja zakonske materije s podzakonskimi predpisi.[3] Nadalje, ne glede na priporočilo URSIV, je vloga Agencije balansirati med predlogi organa s katerim Agencija sodeluje (pri čemer je URSIV nujno bolj varnostno konzervativen organ, saj je njegova vloga zagotavljanje varnosti) in potrebami trga, operaterjev, naročnikov, podjetij in drugih deležnikov. Z razlogom je zakon pooblastilo za sprejem splošnega akta poveril Agenciji, saj bi v primeru uveljavljanja zgolj najstrožjih varnostnih zahtev le-to povsem samostojno lahko opravil URSIV sam.

V zvezi s tem je potrebno ponovno izpostaviti, da je zgolj z uporabo naprednih razlagalnih pravil mogoče izluščiti točne naslovnike oz. zavezance za izpolnjevanje dodatnih varnostnih zahtev. Prvi odstavek 116. člena ZEKom-2[4] 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 uporabo pojma »komunikacijsko omrežje« (med katere spadajo elektronska[5], javna[6], odprta[7]) se (elektronsko) komunikacijsko omrežje, »*Elektronsko komunikacijsko omrežje so sistemi prenosa,[…] ki omogočajo prenos signalov po […] ne glede na vrsto prenesenih informacij.",* razlikuje

[3] Odločba USRS U-I-16/98 z dne 5. 7. 2001, tč. 18; odločba US RS št. U-I-260/09-18 z dne 13. 1. 2011, tč. 6; odločba USRS št. U-I-79/20-24 z dne 13. 5. 2021, tč. 69.
[4] *(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.*
[5] 8. tč. 1. odst. 3. člena ZEKom-2, *Elektronsko komunikacijsko omrežje so sistemi prenosa, ne glede na to, ali temelijijo 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.*
[6] 23. tč. 1. odst. 3. člena ZEKom-2
[7] 48. tč. 1. odst. 3. člena ZEKom-2

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[8] 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 vključil 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.**

2. Znana dejstva in strokovne podlage

Ključna sprememba, ki jo Agencija v novem predlogu sicer uvede, ne pojasni pa ne razlogov za tako odločitev, niti v objavi ni zaznati, ali je bila to ta odločitev, ki jo ima Agencija v mislih, je bolj neposredna opredelitev radijskega omrežja (RAN), kot kritičnega elementa take vrste, da lahko predstavlja predmet presoje in odločitve Vlade RS o prepovedi uporabe.

V nasprotju s tako opredelitvijo pa javno dostopni viri in zadnje stanje tehnike kaže na to, da je taka opredelitev brez strokovne podlage. V skladu z *Nacionalno oceno tveganja kibernetske varnosti 5G v Republiki Sloveniji,*[9] U*sklajeno oceno tveganja EU za kibernetsko varnost omrežij 5G*[10] in *Zbirko orodij EU za kibernetsko varnost omrežij 5G za ukrepe za zmanjšanje tveganja*[11] ("Zbirka orodij EU"), ki so jo

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

[9] Nacionalna ocena tveganja kibernetske varnosti 5G v Republiki Sloveniji je bila pripravljena na podlagi prispevkov 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.

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

[11] 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

pripravile skupine za sodelovanje NIS[12] , ter *dodatkom 5G - k Smernicam o varnostnih ukrepih v okviru EECC*[13] , ki ga je pripravila ENISA (Agencija Evropske unije za kibernetsko varnost), je namreč treba RAN obravnavati kot "HIGH" v primerjavi s CORE in NFV, ki se obravnava kot "CRITICAL". **Na tem mestu torej lahko zgolj ponavljamo, da so varnostne zahteve, ki jih vsebuje Seznam kritičnih**

Slika 1 – Vir: Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, stran 39

-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

sredstev splošnega akta, v nasprotju z viri, ki jih citira navedeni akt in Splošni akt o varnosti omrežij, storitev in podatkov. V zvezi s tem izpostavljamo tudi, da tudi Drugo implementacijsko poročilo[14] ne govori o radijskem omrežju kot kritičnem delu, ne glede na komentarje oz. izjave za novinarje komisarja Bretona, ki so navedeno poročilo spremljali. Navedbe, namenjene novinarjem, so v neposrednem nasprotju z lastnim temeljnim dokumentom »Zbirka Orodij EU«, katerega Implementacijsko poročilo preverja, saj je **prav tam** radijsko dostopovno omrežje opredeljeno kot visoko občutljivo, ne pa kot kritično, kot je npr. jedrni del omrežja.

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

[12] 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).

[13] 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.

[14] https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

orkestracija omrežja NFV. Isto tabelo na strani 39 uporabi Zbirka orodij EU. Razen (populističnih?) in političnih izjav torej ne obstaja niti pravna, niti tehnična podlaga (če pa je, pa bi morala biti razkrita), za vključitev RAN med t.i. »Kritične elemente omrežja«, prav nasprotno, **celoten korpus virov kaže izrecno proti taki vključitvi.**

3. Objektivna metodologija opredelitev kritičnosti

Svetovno sprejeti in široko uporabljani standardi informacijske varnosti predlagajo načine izvajanja ocen tveganj, opredelitev kritičnosti določenega elementa ali sistema, ter na osnovi obojega predlagajo ukrepe in kontrole za obvladovanje tveganj. Na primer Okvir za ocenjevanje tveganj v informacijski varnosti NIST SP 800-53 določa osnovne korake izvajanja ocene tveganj in ukrepov, ki izhajajo iz same ocene:

1. Izvajanje ocene tveganja (Risk Assessment)
2. Izvedena ocena tveganj določi kritičnost posameznega elementa, ki je lahko prizadet zaradi ranljivost, ter določi možne ranljivosti
3. Uvedba ukrepov in kontrol za obvladovanje ugotovljenih tveganj

Kot navedeno zgoraj pod točko 2, standard ETSI/3GPP, tj. TR 121 915 - V.15.0.0 uvaja klasifikacijo omrežnih elementov na osnovi analize tveganj. Zato ni mogoče ugotoviti, na kakšni osnovi predlagani Splošni akt to klasifikacijo spreminja, ne da bi izvedel oceno tveganj in ugotovil odstopanje od uveljavljenih metod, ali od navedenega 3GPP standarda. Prejudiciranje kritičnosti brez opravljene ocene tveganja pa predstavlja nerazumljiv, celo nestrokoven odmik od dobre prakse ali priporočil EU ali ENISE. V zvezi z dejansko, objektivno zaznavno prakso pripominjamo, da ne obstajajo poročila o kakršnihkoli vdorih ali ranljivostih RAN, s katerimi bi se lahko seznanili, v največjem svetovnem poročilu o kibernetskih vdorih za leti 2022 in 2023, *DBIR Verizon 2023 Data Breach Investigations Report | Verizon*,[15] pa ni najti niti enega primera vdora v RAN podsistem kjerkoli po svetu.

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[16], 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*

[15] https://www.verizon.com/business/resources/reports/dbir/

[16] 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

5G ter za tajni nadzor elektronskega komunikacijskega omrežja.[17] Madžarska ne uvaja opredelitve kritičnih omrežnih komponent ali kakršnih koli omejitev.

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

9. 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 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, kar obširno pojasnjuje tudi izr. prof. dr. Samo Bardutzky.

6. Chilling effect

Omejevanje konkurence z oblastnimi akti in dejanji je prepovedano v skladu s 7. poglavjem Zakona o preprečevanju omejevanja konkurence (ZPOmK-2), kjer je potrebno izpostaviti, da ne gre zgolj za akte, temveč tudi dejanja, torej celotno objektivno zaznavno polje obnašanja oblasti. V tem smislu je v skladu z dinamiko tržnih razmer potrebno prav tako izpostaviti, da v primeru najhujših potencialnih omejitev svobodne gospodarske pobude, i.e. prepovedi poslovanja z določenim podjetjem, že sama možnost prepovedi prinaša dejanske gospodarske posledice in vpliva na trg. Racionalni ekonomski akterji na trgu namreč vedno skušajo oceniti in omejitvi tveganje ter na podlagi zaznanih tveganj sprejeti ustrezne poslovne odločitve. V primeru negotovosti je tako racionalna odločitev taka, ki negotovost zmanjša oz. jo omeji na predvidljivo. Odločitev izvršne veje oblasti v zvezi s kritičnimi elementi bi morala biti predvidljiva in osnovana na podlagi strokovnih, vnaprej znanih kriterijev. Ob upoštevanju, da je Agencija že drugič predlagala vključitev RAN med kritične elemente, vsa razpoložljiva relevantna literatura pa kaže, da bi morala ravnati ravno nasprotno, kaže na nepredvidljivost oz. celo arbitrarnost odločanja, ki je tako v svojem bistvu ne-pravno in ne-strokovno. S tem je trgu dan signal, da je potrebno sprejeti ukrepe za omejevanje tveganja, ne glede na to, da npr. še niti ni bil sprejet noben formalni akt, ki bi to tveganje že realiziral.

Izražamo zaskrbljenost, da bi že sama vključitev RAN med kritično infrastrukturo pomenila tržno distorzijo, ki je ne bo mogoče odpraviti, nastala škoda pa bo izmerljiva le v omejenem obsegu v obliki posledic neizogibno ustvarjenega dupoloa, z vsemi negativnimi posledicami, ki jih tak položaj povzroči. Slovenija tako lahko pričakuje višje cene opreme, daljše dobavne roke in omejen nabor tehnologij, upočasnitev razvoja IKT sektorja in s tem zaostajanje digitalizacije narodnega gospodarstva.

[17] 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

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 Seznam kritičnih sredstev prilagodi tako, da 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 Slovenija d.o.o. 1

[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

Kritični elementi omrežja	**Funkcionalnosti omrežja in informacijskih sistemov**
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.
Medomrežno povezovanje	– Funkcije gostovanja in vmesniki do drugih omrežij in storitev
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 in orkestracija 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.~~
Upravljavski sistemi in drugi podporni sistemi	~~– Nadzor delovanja in upravljanja mobilnega komunikacijskega omrežja, vključno z dostopovnim delom (RAN/O-RAN),~~ – Sistemi zaznavanja varnostnih dogodkov, anomalij, groženj in njihovo upravljanje (varnostne funkcije vključno s SIEM/SOAR).
Zakonito prestrezanje	– Funkcije dostopa do vsebine komunikacije in podatkov o prometu uporabnikov s strani pristojnega organa.

telemach

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

1. Na podlagi katerih sprememb na evropski in nacionalni ravni in na podlagi katerih dejstev in ugotovitev, (ki naj bi izhajali iz priporočila Urada Vlade za informacijsko varnost), se je Agencija odločila za vključitev RAN med kritične elemente?

2. 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))?

3. 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)?

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

5. 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?

6. 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.

7. 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)?

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

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