Mnenje Evropskega ekonomsko-socialnega odbora – Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij – Varna uvedba tehnologije 5G v EU – izvajanje nabora orodij EU

(COM(2020) 50 final)

(2020/C 429/37)

Poročevalec: **Alberto MAZZOLA**

Soporočevalec: **Dumitru FORNEA**

Zaprosilo	Evropska komisija, 9. 3. 2020
Pravna podlaga	člen 304 Pogodbe o delovanju Evropske unije
Pristojnost	strokovna skupina za promet, energijo, infrastrukturo in informacijsko družbo
Datum sprejetja mnenja strokovne skupine	3. 9. 2020
Datum sprejetja mnenja na plenarnem zasedanju	16. 9. 2020
Plenarno zasedanje št.	554
Rezultat glasovanja	217/0/2
(za/proti/vzdržani)	

1. **Sklepi in priporočila**

1.1 Evropski ekonomsko-socialni odbor (EESO) pozdravlja pobudo držav članic in Evropske komisije, da se pregleda izvajanje niza ukrepov, priporočenih v sklepnih ugotovitvah iz nabora orodij, ki vključuje strateške, tehnične in ključne ukrepe na področju varnosti pri uvajanju ekosistema 5G v državah članicah.

1.2 EESO meni, da mora ob vse večji kompleksnosti in raznolikosti aplikacij, ki lahko uporabljajo tehnologijo 5G (Evropska komisija je opredelila naslednje cilje povezljivosti za leto 2025: šole, univerze, raziskovalna središča, bolnišnice, glavni izvajalci javnih storitev in digitalno intenzivna podjetja bi morali imeti dostop do prenosa podatkov s hitrostjo 1 Gb/s; gospodinjstva v mestih in na podeželju bi morala imeti dostop do prenosa podatkov s hitrostjo vsaj 100 Mb/s; za vsa mestna območja ter vse glavne ceste in železnice bi morala biti zagotovljena neprekinjena pokritost z omrežji 5G), tovrsten pregled ekosistema 5G, pa tudi ukrepi Evropske komisije za ohranjanje kibernetske varnosti omrežij 5G in raznolike vrednostne verige 5G, tehnične standardizacije in certifikacije, neposrednih tujih naložb ter trgovinske zaščite in varstva konkurence, obveznosti javnih služb, javnih naročil in kibernetske diplomacije, zajemati geopolitično varnost, varnost infrastrukture in podatkov ter zdravstveno varnost, med drugim v smislu člena 168(1) PDEU.

1.3 Po mnenju EESO mora evropski ekosistem omrežja 5G zagotavljati nedotaknjenost, zaupnost, vodstveno in operativno odgovornost, varnost, zamenljivost dobavitelja, interoperabilnost strojne in programske opreme, skupne tehnične in normativne standarde, neprekinjenost storitve, zanesljiv pretok in varstvo podatkov, pokritost vseh območij, tudi redko naseljenih, jasno komunikacijo z uporabnikom kot akterjem na digitalnem trgu ter proaktivno upoštevanje smernic Mednarodne komisije za varstvo pred neionizirajočimi sevanji, da bi zaščitili zdravje prebivalstva in obenem čim bolj zmanjšali sevanje. Zato je Mednarodna komisija za varstvo pred neionizirajočimi sevanji posodobila del smernic iz leta 1998, ki se nanaša na elektromagneta polja radijskih frekvenc. V tem dokumentu (Health Phys. 118(5), 483–524; 2020 – marec 2020) so predstavljene posodobljene smernice, katerih cilj je zaščititi ljudi pred elektromagnetnim sevanjem od 100 kHz do 300 GHz. Mednarodna komisija za varstvo pred neionizirajočimi sevanji (2020) je uvedla vrsto sprememb, da bi zagotovila, da nove tehnologije, kot je 5G, ne glede na naša sedanja pričakovanja ne bi povzročale škode.

1.4 EESO poziva Komisijo, naj skrbno spremlja napredek pri vzpostavljanju in dejanski uporabi omrežja 5G, države članice pa, naj proces še pospešijo, zagotovijo odgovorno izvajanje ter spremljajo vse vidike zanesljivosti in varnosti, med drugim učinke tehnologije 5G na zdravje ljudi in živih ekosistemov, socialno-ekonomske učinke ter učinke na konkurenčnost, vzgojo in izobraževanje, kakor tudi spoštovanje temeljnih pravic.

1.5 EESO meni, da bi morala biti Evropska unija vodilna v svetu na področju naslednje generacije mobilne telefonije 5G in bi morala imeti na voljo varno digitalno infrastrukturo, na kateri bi temeljila nova, sodobna evropska industrijska strategija, ki bi prinesla korenite spremembe na področju mobilne povezljivosti ter bi imela velik potencial za dvig produktivnosti, rast gospodarstva in razvoj storitev za državljane.

1.6 EESO meni, da je zlasti nujno treba zagotoviti ocene profilov tveganja posameznih dobaviteljev in nato uvesti ustrezne omejitve za dobavitelje, ki se štejejo za visoko tvegane, vključno s potrebnimi izključitvami, da bi učinkovito zmanjšali tveganje in določili obveznosti za ključna sredstva, ki so bila opredeljena kot kritična in občutljiva v usklajeni oceni tveganja v EU.

1.7 EESO meni, da si mora Evropa srednjeročno prizadevati za neodvisnost in samozadostnost na tem področju ter odločno podpirati raziskave in različna evropska podjetja. Meni, da je treba povečati sredstva Unije za digitalne raziskave in inovacije ter podpreti naložbe operaterjev in dobaviteljev v nove tehnične in varnostne funkcije. Tovrstne naložbe morajo biti v skladu s sposobnostjo trga, da prepozna in nagradi pobude za povečevanje varnosti in odpornosti sistemov.

1.8 Varnost je treba vsem državam zagotoviti tudi z ohranjanjem raziskovalnih središč na različnih območjih v EU; poleg tega EESO priporoča, da ima vsaka država najmanj dva dobavitelja, od katerih naj bo vsaj eden evropski, kar bi zagotovilo politično varnost podatkov ter spoštovanje zahtev glede zdravstvene ustreznosti.

1.9 Po mnenju EESO je treba poleg ustreznih ukrepov v zvezi s pooblastili nacionalnih regulatorjev in vlogo telekomunikacijskih operaterjev večjo pozornosti nameniti orodjem za uporabnike, državljane in zadevne organizacije civilne družbe, ki so omejena in premalo učinkovita, da bi tako spodbujali opolnomočenje potrošnikov in krepili njihovo vlogo proaktivnih akterjev na trgu.

1.10 Evropska komisija, Evropski parlament, Svet ter vlade in parlamenti držav članic morajo oblikovati demokratičen okvir za posvetovanje, v katerem bi javnosti lahko predstavili znanstvena in tehnična vprašanja, pravna jamstva in odgovore pristojnih institucij na vprašanja civilne družbe.

1.11 EESO priporoča, da se okrepi evropska tehnološka diplomacija, da bi EU omogočila bolj uravnotežene in vzajemne pogoje za trgovino in naložbe, zlasti na področju dostopa podjetij do trga, subvencij, javnih razpisov, prenosa tehnologij, pravic industrijske lastnine ter socialnih in okoljskih predpisov.

2. **Uvod**

2.1 Varnost omrežij 5G je strateškega pomena za državljane in podjetja ter za celoten enotni trg in tehnološko suverenost EU. Komisija je že leta 2013 začela vodilno pobudo EU, v okviru katere je ustanovila javno-zasebno partnerstvo za 5G, da bi pospešila raziskave in inovacije na področju tehnologije 5G.

2.2 Ocenjuje se, da bodo leta 2025 prihodki od omrežij 5G na svetovni ravni znašali več kot 100 milijard EUR, zato je to področje bistvenega pomena za konkurenčnost Evrope na svetovnem trgu, njegova kibernetska varnost pa ključna za zagotavljanje strateške avtonomije Unije.

2.3 Omrežja 5G temeljijo na sedanji četrti generaciji (4G) omrežnih tehnologij in na infrastrukturi optičnega kabla, zagotavljajo nove zmogljivosti ter tako postajajo osrednja infrastruktura in omogočitveni dejavnik za velik del evropskega gospodarstva, ki bo temelj za široko paleto storitev, bistvenih za delovanje notranjega trga ter vzdrževanje in upravljanje ključnih socialnih in ekonomskih dejavnosti, kot so energetika, promet, bančne in zdravstvene storitve ter kmetijski in industrijski procesi proizvodnje, distribucije in potrošnje.

2.4 Zaradi osrednje vloge omrežij 5G pri digitalnem preoblikovanju gospodarstva in družbe EU, medsebojne povezanosti in nadnacionalnosti infrastrukture na podlagi digitalnega ekosistema ter čezmejnosti groženj na tem področju bi morebitne šibke točke in/ali veliki kibernetski incidenti v zvezi z omrežji 5G v eni državi članici vplivali na celotno Unijo. Zato bi bilo treba predvideti ukrepe, ki bodo podlaga za visoko raven skupne kibernetske varnosti omrežij 5G.

2.5 Evropska komisija je leta 2016 v okviru svežnja pobud, ki je vključeval sporočilo o gigabitni povezljivosti za konkurenčen enotni digitalni trg ([1]) ([2]), prenovitev regulativnega okvira za elektronske komunikacije ([3]) in delovanja Organa evropskih regulatorjev za elektronske komunikacije (BEREC) ([4]), prednostne naloge na področju standardizacije IKT za enotni digitalni trg ([5]) ter ukrepe za spodbujanje internetne povezljivosti v lokalnih skupnostih ([6]), sprejela akcijski načrt EU za 5G ([7]), ki ga je EESO pozdravil ([8]). Njegov namen je bil okrepiti prizadevanja EU za vzpostavitev infrastrukture in storitev 5G na enotnem digitalnem trgu s časovnim načrtom za javne in zasebne naložbe v infrastrukturo 5G v EU ter s ciljem zagona komercialnih omrežij 5G do leta 2020.

2.6 V skladu z opredelitvijo iz priporočila Evropske komisije ([9]) „omrežja 5G“ pomenijo „sklop vseh relevantnih elementov omrežne infrastrukture za mobilno in brezžično komunikacijsko tehnologijo, ki se uporabljajo za povezljivost in storitve dodane vrednosti, z značilnostmi naprednega delovanja, kot so zelo velika hitrost prenosa podatkov in zmogljivost, komunikacije z nizko stopnjo zakasnitve, ultravisoka stopnja zanesljivosti ali podpiranje številnih povezanih naprav“.

2.7 V priporočilu je navedeno, da bo Komisija podprla izvajanje pristopa EU h kibernetski varnosti omrežij 5G in si bo v skladu z zahtevo držav članic prizadevala za zagotovitev varnosti infrastrukture 5G in dobavne verige, pri čemer bo po potrebi uporabila vsa orodja, ki jih ima na voljo:

— pravila s področja telekomunikacij, multimedijskih storitev in kibernetske varnosti,

— usklajevanje glede standardizacije in certifikacije na ravni EU,

— okvir za pregledovanje neposrednih tujih naložb za zaščito dobavne verige evropskega 5G,

— instrumente trgovinske zaščite,

— pravila konkurence,

— javna naročila, pri čemer si bo prizadevala zagotoviti ustrezno upoštevanje varnostnih vidikov,

— programe financiranja EU, pri čemer bo zagotavljala, da bodo upravičenci izpolnjevali ustrezne varnostne zahteve.

2.8 Države članice so julija 2019 skupini za sodelovanje, ki je bila ustanovljena v skladu z direktivo o omrežjih in informacijskih sistemih ([10]) in jo sestavljajo predstavniki iz vseh držav članic, Evropski komisiji in Agenciji Evropske unije za kibernetsko varnost (ENISA) predstavile rezultate svojih nacionalnih ocen tveganja, ki so vsebovali informacije o glavnih dejavnostih, grožnjah in šibkih točkah v skladu s standardom ISO/IEC 27005 v povezavi z infrastrukturo 5G in z glavnimi scenariji tveganja ter opis možnih načinov, na katere bi akterji groženj lahko izkoristili šibke točke posameznih dejavnosti. Te nacionalne ocene tveganja so bile podlaga za nadaljnjo usklajeno oceno in za skupen nabor orodij z možnimi ukrepi za zmanjševanje tveganja.

2.9 Skupina za sodelovanje na področju varnosti omrežij in informacij je oktobra 2019 ob podpori Evropske komisije in agencije ENISA predstavila poročilo o usklajeni oceni tveganja v EU za kibernetsko varnost omrežij 5G, v kateri so bili opredeljeni številni pomembni varnostni izzivi, povezani s ključnimi tehnološkimi inovacijami na področju programske opreme, aplikacij in storitev, z vlogo dobaviteljev pri vzpostavitvi in uporabi omrežij 5G ter s stopnjo odvisnosti od posameznih dobaviteljev:

— večja izpostavljenost napadom in večje število možnih vstopnih točk za napadalce,

— večja občutljivost zaradi novih lastnosti arhitekture omrežij 5G in njihovih funkcij,

— odvisnost omrežnih operaterjev mobilne telefonije od dobaviteljev in povečano število napadnih poti, ki bi jih lahko izkoristili akterji groženj,

---

([1]) Člen 168(1) PDEU: „Dejavnost Unije, ki dopolnjuje nacionalne politike, […]“
([2]) COM(2016) 587.
([3]) COM(2016) 590.
([4]) COM(2016) 591.
([5]) COM(2016) 176.
([6]) COM(2016) 589.
([7]) COM(2016) 588.
([8]) UL C 125, 21.4.2017, str. 74.
([9]) Priporočilo Komisije (EU) 2019/534 z dne 26. marca 2019, *Kibernetska varnost omrežij 5G* (UL L 88, 29.3.2019, str. 42).
([10]) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

— pomen profila tveganja posameznih dobaviteljev zaradi možnosti vmešavanja akterjev iz tretjih držav,

— povečano tveganje za morebitne prekinitve dobave zaradi napetosti na področju trgovine ali drugih razlogov, ki izhaja iz velike odvisnosti od dobaviteljev,

— nevarnost za razpoložljivost in nedotaknjenost omrežij z vidika varnosti, zaupnosti in zasebnosti.

2.10 Vsi ti izzivi ustvarjajo novo varnostno paradigmo, saj je treba zaradi njih ponovno oceniti sedanji politični in varnostni okvir, ki se uporablja za ta sektor in njegov ekosistem, države članice pa morajo sprejeti ustrezne ukrepe za zmanjšanje tveganja.

2.11 Agencija ENISA je 21. novembra 2019 objavila poročilo o pregledu groženj, povezanih z omrežji 5G, v katerem je ocenila grožnje, povezane s peto generacijo omrežij za mobilne telekomunikacije, in vanj vključila tudi poročilo držav članic EU.

2.12 Skupina za sodelovanje na področju varnosti omrežij in informacij je 29. januarja 2020 objavila dokument z naslovom *Cybersecurity of 5G networks – EU toolbox of risk mitigating measures* ([11]) (Kibernetska varnost omrežij 5G – nabor orodij EU za zmanjševanje tveganja), v katerem so navedeni nabor možnih skupnih ukrepov za zmanjševanje glavnih tveganj na področju kibernetske varnosti omrežij 5G ter smernice za izbor prednostnih ukrepov v načrtih za zmanjšanje tveganja na nacionalni ravni in na ravni EU. Istega dne je Evropska komisija sprejela sporočilo v podporo naboru orodij ([12]), ki je predmet tega mnenja.

2.13 Glavni deležniki v infrastrukturi omrežij 5G so:

— državljani, potrošniki in končni uporabniki 5G,

— operaterji mobilnih omrežij: subjekti, ki zagotavljajo storitve mobilnega omrežja uporabnikom in pri tem upravljajo svoje omrežje s pomočjo tretjih oseb,

— dobavitelji operaterjev mobilnih omrežij: subjekti, ki operaterjem mobilnih omrežij zagotavljajo storitve ali infrastrukturo za izgradnjo ali upravljanje njihovih lastnih omrežij. Ta kategorija zajema proizvajalce telekomunikacijske opreme in druge tretje ponudnike, kot so ponudniki storitev v oblaku, sistemski integratorji, podizvajalci za varnost in vzdrževanje ter proizvajalci opreme za prenos,

— proizvajalci povezanih naprav in zadevni dobavitelji storitev: subjekti, ki dobavljajo predmete ali storitve, ki se bodo povezale z omrežji 5G (npr. pametni telefoni, povezana vozila, e-zdravje), in ustrezne storitve iz nadzorne ravnine 5G, kot je opredeljena z arhitekturo, temelječo na storitvah ali mobilnem računalništvu na robu,

— drugi deležniki, med drugim dobavitelji storitev in vsebin.

Vsi ti deležniki so pomembno povezani z varnostjo, z vidika prispevanja k informacijski varnosti omrežij 5G ali kot morebitne vstopne točke oziroma napadni vektorji. Zato je treba oceniti tveganja, povezana z njihovim položajem v ekosistemu 5G.

2.14 Glavne klasične kategorije nevarnosti so povezane z ogrožanjem zaupnosti, nedotaknjenosti in razpoložljivosti. Natančneje je bilo ugotovljeno, da vrsta scenarijev nevarnosti za omrežja 5G zadeva zlasti:

— prekinitve v lokalnem ali globalnem omrežju 5G (razpoložljivost),

— vohunjenje pri podatkovnem prometu v infrastrukturi omrežja 5G (zaupnost),

— spreminjanje ali preusmeritev podatkovnega prometa v infrastrukturi omrežja 5G (nedotaknjenost in/ali zaupnost),

— uničenje ali spreminjanje druge digitalne informacijske infrastrukture ali sistemov prek omrežij 5G (nedotaknjenost in/ali razpoložljivost).

2.15 Grožnje, ki jih predstavljajo države ali akterji s podporo držav, veljajo za zelo pomembne, saj so to najresnejši in najverjetnejši akterji groženj, ki imajo lahko motiv, namen in zlasti sposobnost za izvajanje ponavljajočih se in izpopolnjenih napadov na varnost omrežij 5G.

([11]) https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5 g-networks-eu-toolbox-risk-mitigating-measures.
([12]) https://ec.europa.eu/digital-single-market/en/news/secure-5 g-deployment-eu-implementing-eu-toolbox-communication-commission.

Čeprav mnoge izmed teh šibkih točk niso značilne le za omrežja 5G, je verjetno, da se bosta z uvedbo 5G njihovo število in pomen povečala zaradi večje kompleksnosti tehnologije in zaradi večje odvisnosti gospodarstev in družb od te infrastrukture v prihodnosti.

2.16 Ker bodo omrežja 5G v veliki meri temeljila na programski opremi, bi glavne pomanjkljivosti glede varnosti, na primer tiste, ki izhajajo iz slabih procesov pri razvoju programske opreme pri dobaviteljih naprav, akterjem lahko olajšale namerno vgraditev stranskih vrat, zaradi česar bi jih bilo še teže odkriti. Tako se lahko poveča možnost, da bi imelo njihovo izkoriščanje posebno resne in razširjene negativne učinke. Medtem ko problemi kibernetske varnosti pri 4G še vedno niso rešeni, bodo problemi pri 5G lahko eksponentno naraščali.

2.17 Upoštevati je treba šibke točke, povezane s procesom, in tiste, povezane s konfiguracijo:

— pomanjkanje specializiranega kadra, usposobljenega za varovanje, spremljanje in vzdrževanje omrežij 5G,

— pomanjkljivosti v ustreznih notranjih varnostnih kontrolah, spremljanju, sistemih za upravljanje varnosti ter upravljanju tveganj,

— neustreznost varnostnih postopkov ali postopkov operativnega vzdrževanja, kot so posodabljanje programske opreme ali upravljanje popravkov v omrežjih 5G,

— neskladnost s standardi 3GPP ali napačno izvajanje standardov,

— pomanjkljivosti v zasnovi ali arhitekturi omrežja, med drugim pomanjkanje učinkovitih mehanizmov za izredne razmere in neprekinjeno delovanje, neustrezna ali napačna konfiguracija, na primer pri virtualizaciji ali pri pravicah za upravljanje ali dostop,

— neustrezna merila za lokalni dostop in dostop na daljavo do sestavnih delov omrežja,

— neustreznost varnostnih zahtev v postopku dobave; pri tej šibki točki gre lahko za neustrezne strategije pri izbiri dobaviteljev ali za dajanje prednosti drugim vidikom pred varnostjo.

2.18 Pri ocenjevanju profilov tveganja posameznih dobaviteljev je treba upoštevati več dejavnikov, zlasti: možnost, da je dobavitelj pod vplivom tretje države zaradi močnih povezav med njim in vlado tretje države; zakonodajo tretje države, zlasti če niso v veljavi zakonodajni ali demokratični mehanizmi za nadzor in ravnotežje in če posledično hčerinske družbe, ki delujejo v EU, ne spoštujejo zakonodaje EU, ali če med EU in zadevno tretjo državo ni podpisan sporazum o varnosti ali varstvu podatkov; značilnosti lastništva dobavitelja; sposobnost tretje države, da izvaja kakršno koli obliko pritiska, med drugim v povezavi s krajem proizvodnje opreme; splošno kakovost proizvodov in dobaviteljevo ravnanje na področju kibernetske varnosti, vključno s stopnjo nadzora nad lastno dobavno verigo in ustreznim prednostnim obravnavanjem varnosti.

2.19 Države članice so se strinjale, da bodo zagotovile ukrepe, ki bodo omogočali ustrezen in sorazmeren odziv na že ugotovljena tveganja ter na morebitna prihodnja tveganja. Zlasti so se strinjale, da morajo zagotoviti, da bodo s pristopom na podlagi tveganja sposobne omejiti, prepovedati in/ali naložiti posebne zahteve in pogoje za dobavo, uvedbo in delovanje opreme za omrežje 5G.

2.20 V tem smislu bi države članice morale zagotoviti:

— krepitev varnostnih zahtev za omrežne operaterje mobilne telefonije, kot so strog nadzor nad pristopom, pravila za varno delovanje in spremljanje, omejitve zunanjega izvajanja določenih funkcij itd.,

— ocene profilov tveganja dobaviteljev na podlagi objektivnih in jasnih meril; posledično uvedba ustreznih omejitev v skladu z načeli sorazmernosti in pravne varnosti za dobavitelje, ki štejejo za visoko tvegane, vključno s potrebnimi izključitvami, da bi učinkovito zmanjšali tveganje za ključna sredstva, opredeljena kot kritična in občutljiva v usklajeni oceni tveganja v EU,

— izvajanje splošno priznanih in uveljavljenih varnostnih standardov in najboljših praks, ki temeljijo na soglasju,

— da bo imel vsak operater ustrezno večdobaviteljsko strategijo, da se bo izognil preveliki odvisnosti od enega samega dobavitelja ali dobaviteljev s podobnim profilom tveganja,

— strog nadzor nad varnim dostopom, upravljanjem, delovanjem in spremljanjem omrežja ter nad uporabo certificiranja za opremo in/ali postopke za omrežje 5G. Ta strategija mora temeljiti na analizi tveganja, ki jo izvedejo države članice in operaterji, tako da se z izbiro strategije več prodajalcev ne poveča raven tveganja za operaterjevo omrežje,

— primerno ravnotežje dobaviteljev na nacionalni ravni in preprečevanje odvisnosti od dobaviteljev, ki se štejejo za visoko tvegane, tudi s spodbujanem večje interoperabilnosti opreme,

— vzdrževanje raznolike in trajnostne dobavne verige 5G, da bi preprečile dolgoročno odvisnost, tako da bodo v celoti izkoristile obstoječa orodja in instrumente EU za nadzor neposrednih tujih naložb, instrumente trgovinske zaščite ter pravila konkurence in pravila EU na področju javnih naročil,

— krepitev notranjih zmogljivosti EU na področju tehnologij 5G in tehnologij naslednic 5G z uporabo ustreznih programov in sredstev EU, usklajevanjem med državami članicami glede standardizacije s krepitvijo zmogljivosti za preizkušanje in nadzor, da bi dosegle določene varnostne cilje in razvile ustrezne certifikacijske sheme za vso EU v skladu z zakonodajo na področju informacijske varnosti in spodbujanjem interoperabilnosti.

2.21 Evropska komisija je ob več priložnostih poudarila, da je notranji evropski trg vedno odprt za tiste, ki želijo vstopiti v Evropo, pod pogojem, da izpolnjujejo jasna in zahtevna pravila na podlagi objektivnih meril.

2.22 Svet je 6. junija 2020 poudaril pomen krepitve suverenosti in sodelovanja na področju digitalne tehnologije v EU ter ustvarjanja sinergij s programi EU, kot sta Instrument za povezovanje Evrope ter program za digitalno Evropo, z razvojem digitalnih kompetenc, gospodarstva podatkov, pomena umetne inteligence in informacijske varnosti ter z aktivno vlogo digitalne tehnologije pri doseganju ciljev zelenega dogovora.

3. **Sporočilo Evropske komisije**

3.1 Komisija v odgovor na dokument skupine za sodelovanje na področju varnosti omrežij in informacij o naboru orodij EU za kibernetsko varnost 5G:

— si v skladu z zahtevami držav članic prizadeva za zagotavljanje varnosti infrastrukture 5G in dobavne verige, pri čemer po potrebi uporablja vsa razpoložljiva orodja,

— poziva države članice in institucije, naj zagotovijo izvajanje učinkovitih strategij za zmanjševanje tveganj ter sprejmejo dodatne ukrepe za usklajevanje na ravni EU in s tem oblikujejo skupen pristop h kibernetski varnosti 5G,

— poziva države članice, naj nadaljujejo izvajanje ukrepov, priporočenih v sklepnih ugotovitvah v naboru orodij, ter pripravijo skupno poročilo o izvajanju, skupina za sodelovanje na področju varnosti omrežij in informacij pa bo nadaljevala z delom v podporo izvajanju tega nabora,

— na področjih, za katera je pristojna, predvideva dejavnosti ohranjanja kibernetske varnosti omrežij 5G in raznolike vrednostne verige 5G, tehnične standardizacije in certifikacije, neposrednih tujih naložb, trgovinske zaščite in konkurence, javnih naročil in kibernetske diplomacije, pa tudi lastne programe in z njimi povezana sredstva, zlasti za raziskave in inovacije, kohezijo ter razvoj.

4. **Splošne ugotovitve**

4.1 EESO je prepričan, da lahko nove tehnologije 5G spremenijo naš način povezovanja s svetom in ponudijo možnosti za nove aplikacije, poslovne modele, nove življenjske sloge, pametne tovarne, večjo produktivnost in nove kakovostne storitve za državljane ter lahko odprejo vrata revolucionarnim tehnologijam, kot so avtomatizirani avtomobili ter napredni sistemi za proizvodnjo in distribucijo, poleg tega pa lahko omogočijo medsebojno povezovanje na tisoče naprav, ki bodo kot elementi interneta stvari postale del našega vsakdana. Kljub vsemu pa EESO pričakuje, da bo Evropska komisija okrepila študije izvedljivosti ter analize stroškov in koristi 5G v primerjavi z uporabo tehnologije 4G ali telekomunikacij preko optičnega kabla. EESO meni, da je bistveno, da je 5G usmerjen k boljši krožni rabi virov, da se zmanjša velik delež ogljičnega odtisa, ki je povezan z energijo. EESO poudarja, da je treba socialne strukturne spremembe obravnavati s spodbujanjem pravičnega in nemotenega prehoda ter odpravljanjem vrzeli v znanju in spretnostih, da bi dosegli boljše plačane, prožnejše in visokokvalificirane zaposlitve.

4.2 Sedanja trojna grožnja – nenadzorovana pandemija, nezadostni instrumenti ekonomske politike in geopolitični „črni labodi“ – bi lahko svetovno gospodarstvo pahnila v dolgotrajno recesijo ter povzročila zlom finančnega trga in beg z njega ravno v trenutku, ko se vsi segmenti evropske družbe začenjajo vse bolj zavedati, da so za trajnostni gospodarski razvoj **in za digitalno revolucijo, ki se je že začela in katere bistveno orodje je 5G**, potrebni tehnološka suverenost, rast produktivnosti in učinkovitejša raba razpoložljivih virov. Zanje pa je potrebna podpora ustreznega pravno-regulativnega in ekonomsko-finančnega okvira.

4.3 EESO poziva institucije EU in države članice, naj dokončajo evropski enotni digitalni trg, vključno z razvojem zmogljivosti za vključitev in uporabo storitev 5G, da bi zaščitili in izboljšali konkurenčnost evropske industrije. Evropsko komisijo poziva, naj strogo nadzoruje napredek pri vzpostavljanju in dejanski uporabi 5G, države članice pa, naj dodatno pospešijo ta proces, pri čemer naj upoštevajo vse vidike zanesljivosti in varnosti, med drugim učinke tehnologij 5G na zdravje ljudi in živih ekosistemov, socialno-ekonomske učinke, učinke na konkurenčnost, izobraževanje in usposabljanje ter zagotavljanje spoštovanja temeljnih pravic, kot so pravice do lastnine, zasebnosti in varnosti osebnih podatkov.

4.4 EESO meni, da bi morala biti Evropska unija vodilna v svetu na področju naslednje generacije mobilne telefonije 5G in bi morala imeti na voljo varno digitalno infrastrukturo, na kateri bi temeljila nova, sodobna evropska industrijska strategija. Ta bi prinesla korenite spremembe na področju mobilne povezljivosti in velik potencial za dvig produktivnosti, rast gospodarstva in razvoj storitev za državljane, njihovo blaginjo, varstvo podnebja in okolja ter bi EU postavila na čelo revolucije 5G.

4.5 Ker sta kibernetska varnost in državna varnost med seboj neločljivo povezani, EESO meni, da mora biti vsaka odločitev države članice EU glede državne varnosti sprejeta ob upoštevanju okoliščin v EU, ocene, ki niso tehnične narave, pa je treba objektivno izvesti na podlagi meril za oceno tveganja, opredeljenih na evropski ravni, s čimer bi zagotovili predvidljivo in po vsej Evropi usklajeno regulativno okolje, ki bi omogočalo polno interoperabilnost.

4.6 EESO meni, da kakovost informacij in sredstva komunikacije – t. i. uokvirjanje (učinek konteksta ali postavljanja na pomembno mesto ali opaznost) – znatno vplivajo na vedenje naslovnikov. Zato je za izpolnitev cilja opolnomočenja potrošnikov treba opredeliti orodja za njihovo izobraževanje in krepitev njihovih sposobnosti, da bodo imeli aktivno vlogo na digitalnem trgu. EESO ugotavlja, da je treba državljanom zagotavljati ažurne in točne informacije o koristih in tveganjih 5G, ki bodo temeljile na soglasju velike večine znanstvene skupnosti in bodo nakazovale tudi vidike, glede katerih ni jasnega soglasja.

4.7 EESO je prepričan, da mora biti dostop do evropskega digitalnega trga še naprej prost za vsa podjetja, brez diskriminacije, vendar ob upoštevanju evropskega okvira neomajnih in jasnih pravil, standardov in meril za ocenjevanje in varnost, ki bi v središče evropske strategije postavljala ponovno vzpostavitev evropske tehnološke suverenosti.

4.8 Med petimi glavnimi dobavitelji infrastrukture sta dve evropski podjetji, dve kitajski in eno korejsko ([13]). Nobenega evropskega podjetja pa ni med glavnimi proizvajalci naprav in sistemskih naborov čipov 5G. EESO je prepričan, da je treba zagotoviti prisotnost več dobaviteljev, od katerih mora najmanj eden imeti matično družbo v Evropi, ter okvir za interoperabilnost in polno zamenljivost strojne in programske opreme, tudi zato, da se zagotovi polna tehnološka suverenost Evrope v okviru tesnega mednarodnega sodelovanja in polne vzajemne odprtosti, dostopnosti in delovanja na trgih. Takšna raznolikost je možna, dokler je mogoča interoperabilnost storitev in se tveganja za kibernetsko varnost zaradi nje ne večajo.

4.9 EESO meni, da si mora Evropa srednjeročno prizadevati za neodvisnost in samozadostnost na tem področju ter odločno podpirati raziskave in različna evropska podjetja. EESO pozdravlja sveženj ukrepov, dogovorjen med državami članicami za obravnavanje varnostnih tveganj, povezanih z uvedbo tehnologije 5G, ki so bila opredeljena v evropski oceni tveganja. Vendar meni, da je treba za vse frekvenčne pasove, predvidene za 5G ([14]), uporabljati stroge in varne omejitve izpostavljenosti elektromagnetnim poljem, kot so bile priporočene na ravni EU na podlagi posodobljenih smernic Mednarodne komisije za varstvo pred neionizirajočimi sevanji, ki jih priznava tudi Svetovna zdravstvena organizacija. Omejitve, ki jih je predlagala Mednarodna komisija za varstvo pred neionizirajočimi sevanji, temeljijo na previdnostnem načelu, saj so 50-krat nižje od vrednosti, ki so bile ugotovljene kot škodljive za zdravje ljudi na podlagi razpoložljivih znanstvenih dokazov.

([13]) Glavni svetovni dobavitelji so trenutno Ericsson, Nokia, Huawei, ZTE in Samsung.
([14]) EP – E-003040/2019 – Odgovor je podala Stela Kiriakides v imenu Evropske komisije (17. 1. 2020).

4.10 Vendar EESO ugotavlja, da smernic Mednarodne komisije za varstvo pred neionizirajočimi sevanji ne priznava celotna znanstvena skupnost, saj se nekateri znanstveniki zavzemajo za veliko strožje omejitve izpostavljenosti ljudi sevanju v skladu z načelom „tako nizko, kakor je to mogoče doseči z uporabo razumnih ukrepov“ . Rešitve, ki bi jih lahko predlagali za dopolnitev komunikacijske infrastrukture 5G zajemajo uporabo fiksnih podatkovnih priključkov z uporabo obstoječih tehnologij brez sevanja (ethernetni kabli, optična vlakna itd.) za neprenosno uporabo (npr. pri bankomatih, v bančnih poslovalnicah, za industrijske robote, za medicinske robote, ki se upravljajo na daljavo itd.) ter v sektorjih, kjer operaterji prenašajo velike količine podatkov (ponudniki digitalnih storitev, podjetja/družbe itd.); in uporabo interneta stvari na fiksnih, neprenosnih mestih (pametne hiše, pametna mesta, senzorji na infrastrukturi javnih storitev itd.).

4.11 Evropska komisija, Evropski parlament, Svet ter vlade in parlamenti držav članic morajo oblikovati demokratičen okvir za posvetovanje, v katerem bi javnosti lahko predstavili znanstvena in tehnična vprašanja, pravna jamstva in odgovore pristojnih institucij na vprašanja civilne družbe.

4.12 Po mnenju EESO je treba poleg ustreznih ukrepov v zvezi s pooblastili nacionalnih regulatorjev in vlogo telekomunikacijskih operaterjev večjo pozornost nameniti orodjem za uporabnike, državljane in zadevne organizacije civilne družbe, ki so omejena in premalo učinkovita.

4.13 EESO je priznal ([15]) obstoj problema preobčutljivosti na elektromagnetna sevanja in navedel razloge za svojo zaskrbljenost. Obenem je kot spodbudno ocenil, da potekajo nadaljnje poglobljene raziskave, da bi razumeli problem in njegove vzroke, ter pozval Komisijo, naj nadaljuje in posodobi prizadevanja na tem področju.

4.14 Verodostojnost dobaviteljev telekomunikacijskih in aplikacijskih storitev 5G je po mnenju EESO bistvena, saj je upravljanje informacij na internetu temelj storitev zbirnih podatkov, ki se zbirajo pri uporabnikih in obdelujejo v skladu s tehnološkimi, pravnimi in fiskalnimi mehanizmi in ob neposredni medsebojni povezanosti predmetov, strojev in algoritmov.

4.15 EESO je predlagal ([16]) prehod od koncepta lastništva podatkov k opredelitvi pravic do podatkov za fizične osebe in pravne osebe. Potrošniki bi morali imeti pravico do podatkov, ki jih proizvedejo povezane naprave, tako, da bi bila zagotovljena zasebnost potrošnikov pri dostopu, interoperabilnosti in prenosu podatkov, obenem pa tudi ustrezna varnost in zaupnost podatkov, lojalna konkurenca ter večja izbira za potrošnike.

4.16 Splošno uredbo o varstvu podatkov bi bilo treba dopolniti z jasnimi smernicami za uporabo, da bi ob medsebojni povezanosti naprav in predmetov zagotovili enotno uporabo ter visoko raven varstva podatkov in potrošnikov. Poleg tega bi bilo treba pregledati pravila o civilni odgovornosti in zavarovanju proizvodov ter jih prilagoditi položaju, v katerem bo vse več odločitev sprejemala programska oprema v popolnoma varnem okolju.

4.17 EESO meni, da morajo države članice upoštevati strateška in tehnična priporočila iz nabora orodij EU in se izogibati oblikovanju posebnih nacionalnih pristopov, na primer dodatnih preskusov in certificiranj, ki bi povzročili drobitev trga, zamude pri uvajanju tehnologij in neskladnosti med trgi, to pa bi lahko ogrozilo zaupanje v sisteme preskušanja in certificiranja.

4.18 EESO meni, da je pomembno uporabiti svetovne standarde, ki imajo v Evropi vse večjo podporo, ter skupne in priznane primere dobre prakse, da bi omogočili učinkovito obvladovanje groženj, vzpostavitev ekonomije obsega, izogibanje razdrobljenosti in zagotavljanje interoperabilnosti evropskih sistemov. Razjasniti je treba nekatere vidike tehničnih standardov, saj bo to podjetjem omogočilo konkurenčnost in opravljanje teh temeljnih dejavnosti, ki omogočajo uporabo naprednih tehnologij, kot sta 5G in umetna inteligenca, na vseh trgih.

4.19 EESO meni, da je zlasti nujno treba zagotoviti ocene profilov tveganja posameznih dobaviteljev in nato uvesti ustrezne omejitve za dobavitelje, ki se štejejo za visoko tvegane, vključno s potrebnimi izključitvami, da bi učinkovito zmanjšali tveganje za ključna sredstva, opredeljena kot kritična in občutljiva v usklajeni oceni tveganja v EU.

4.20 EESO meni, da je treba povečati naložbe operaterjev in dobaviteljev v nove tehnične in varnostne funkcije. Tovrstne naložbe morajo biti v skladu s sposobnostjo trga, da prepozna in nagradi vse pobude, namenjene povečevanju varnosti in odpornosti sistemov. Večja vidnost naložb v varnost bi lahko omogočila nove oblike nagrajevanja na trgu.

([15]) UL C 242, 2.7.2015, str. 31.
([16]) UL C 353, 18.10.2019, str. 79.

4.21 EESO odločno podpira skupne ukrepe v podporo industrijskemu razvoju in uvajanju tehnologije 5G, kot so ocenjevanje možnih tržnih vrzeli vzdolž vrednostne verige 5G, ki bi upravičile ciljno usmerjene intervencije v okviru naslednjega dolgoročnega proračuna ali morda pomembnih projektov skupnega evropskega interesa na področju kibernetske varnosti 5G (zanesljivost in varnost).

4.22 EESO poudarja, da se je digitalna infrastruktura med krizo zaradi COVID-19 sicer izkazala kot odporna in stabilna, kljub temu pa so potrebne nadaljnje naložbe v infrastrukturo 5G, da bi presegli še vedno obstoječi digitalni razkorak, ki lahko omejuje dostop državljanov do e-zdravja, e-učenja in dela na daljavo.

4.23 V povezavi s tehnološko diplomacijo EESO meni, da mora EU, zlasti zaradi prisotnosti sistemskih konkurentov, ki spodbujajo drugačne oblike upravljanja, zagotoviti bolj uravnotežene in vzajemne pogoje za trgovino in naložbe, predvsem na področju dostopa podjetij do trga, subvencij, javnih naročil, prenosa tehnologij, pravic industrijske lastnine ter socialnih in okoljskih predpisov, obenem pa mora spodbujati popolno konkurenco in tehnične inovacije na trgu.

4.24 EESO odločno podpira potrebo po vzdrževanju raznolike in trajnostne dobavne verige 5G, da bi preprečili dolgoročno odvisnost, za kar je treba zagotoviti prisotnost več dobaviteljev ter zamenljivost in interoperabilnost, v večletnem finančnem okviru 2021–2027 pa dodatno okrepiti programe in pobude za krepitev zmogljivosti in suverenosti EU na področju tehnologij 5G in tehnologij naslednic 5G.

4.25 V okviru načrta okrevanja za Evropo, ki je bil sprejet 27. maja 2020, bodo na podlagi indeksa digitalnega gospodarstva in družbe (DESI) za leto 2020 opravljene posebne analize za posamezne države v podporo priporočilom evropskega semestra za digitalno preobrazbo. To bo državam članicam v pomoč pri opredelitvi in prednostnem razvrščanju njihovih potreb po reformah in naložbah ter jim tako olajšalo dostop do mehanizma za okrevanje in odpornost v vrednosti 560 milijard EUR. S sredstvi iz tega mehanizma bodo države članice okrepile svoja gospodarstva ter zagotovile, da bodo naložbe in reforme podpirale zeleni in digitalni prehod. Ker je pandemija znatno vplivala na vseh pet razsežnosti indeksa DESI, bi bilo treba sklepe za leto 2020 glede 5G obravnavati v povezavi s številnimi ukrepi, ki so jih sprejele Evropska komisija in države članice za upravljanje krize in v podporo okrevanju.

V Bruslju, 16. septembra 2020

Predsednik
Evropskega ekonomsko-socialnega odbora
Luca JAHIER