Uloga dobavljača opreme u sigurnosti 5G mreže

Matić, Katarina

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Katarina Matić

ULOGA DOBAVLJAČA OPREME U SIGURNOSTI 5G MREŽE

SPECIJALISTIČKI RAD

Zagreb, 2023.

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING
SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Katarina Matić

THE ROLE OF EQUIPMENT VENDORS IN 5G NETWORK SECURITY

ULOGA DOBAVLJAČA OPREME U SIGURNOSTI 5G MREŽE

SPECIALIST THESIS
SPECIJALISTIČKI RAD

Zagreb, 2023.

Završni specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva, na Zavodu za elektroniku, mikroelektroniku, računalne i inteligentne sustave.

Mentor: izv. prof. dr. sc. Stjepan Groš

Završni rad ima: 66 stranica

Završni rad br.: _____

Povjerenstvo za ocjenu u sastavu:

1. izv. prof. dr. sc. Marin Vuković – predsjednik
2. izv. prof. dr. sc. Stjepan Groš – mentor
3. izv. prof. dr. sc. Toni Perković, Sveučilište u Splitu Fakultet elektrotehnike, strojarstva i brodogradnje – član

Povjerenstvo za obranu u sastavu:

1. izv. prof. dr. sc. Marin Vuković – predsjednik
2. izv. prof. doc. dr. sc. Stjepan Groš – mentor
3. izv. prof. dr. sc. Toni Perković, Sveučilište u Splitu Fakultet elektrotehnike, strojarstva i brodogradnje – član

Datum obrane: 23. veljače 2023.

Sažetak

Karakteristike pete generacije mobilnih mreža (5G) i zabrana korištenja opreme kineskih dobavljača u Australiji, Japanu, SAD-u i drugim zemljama bili su motivirajući faktori za proučavanje utjecaja dobavljača opreme na sigurnost 5G mreže i pisanje ovog rada.

Opremu kineskih dobavljača sve veći broj zemalja smatra visokorizičnom pa je tako i u Europskoj Uniji preporuka izbjegavati njenu uporabu jer može ugroziti sigurnost 5G mreže. Utjecaj Kine na kineske tvrtke je značajan, zakonom je propisano osnivanje organizacije Komunističke partije i provođenje nadzora u tvrtkama te dostava zatraženih informacija. Huawei je najveći kineski dobavljač 5G opreme i iako se nastoji prilagoditi sigurnosnim zahtjevima zapadnih zemalja i mnogo ulaže u razvoj i sigurnost svoje opreme i usluga, podliježe kineskim zakonima i smatra se visokorizičnim.

Cilj rada je opisati 5G tehnologiju, 5G sigurnosnu arhitekturu, vodeće dobavljače opreme s naglaskom na one visokorizične te mjere koje bi operatori trebali uzeti u obzir kod odabira dobavljača, s ciljem očuvanja povjerljivosti, cjelovitosti i dostupnosti podataka u prijenosu, obradi i pohrani.

Ključne riječi: 5G, jezgrena mreža, radio pristupna mreža, virtualizacija, dijeljenje mrežnih resursa, ranjivosti, prijetnje, rizici, Kina, Toolbox, Huawei, Ericsson, Nokia

Summary

Fifth-generation mobile networks (5G) characteristics and the ban on the use of Chinese suppliers equipment in Australia, Japan, USA and other countries were motivating factors for studying the influence of equipment suppliers on 5G network security and writing this paper.

An increasing number of countries considers Chinese suppliers equipment high-risk. EU recommends avoiding its use in its Member States as it can endanger 5G network security. The influence of China on Chinese companies is significant, the law prescribes the establishment of the Communist Party, carrying out supervision in companies and delivery of requested information. Huawei is China's largest 5G equipment supplier and although it strives to adapt to the security requirements of Western countries and invests heavily in the development and security of its equipment and services, it is subject to Chinese laws and is considered high-risk.

The aim of the work is to describe 5G technology, 5G security architecture, leading equipment suppliers with an emphasis on high-risk ones and measures operators should take into account when choosing suppliers, with the aim of maintaining the confidentiality, integrity and availability of data while stored, processed and handled.

Key words: 5G, core network, radio access network, virtualization, network slice, vulnerabilities, threats, risks, China, Toolbox, Huawei, Ericsson, Nokia

Sadržaj

1. Uvod

Otprilike svakih deset godina implementira se nova generacija mobilnih mreža. Tako se od 2018. uvodi peta generacija koju karakteriziraju velike propusne brzine, malo kašnjenje, visoka pouzdanost i velik broj spojenih različitih bežičnih uređaja. Očekuje se kako će 5G biti osnova za razvoj gospodarstva i novih rješenja koja će poboljšati kvalitetu života. Pametni gradovi će pomoću 5G-a moći prilagoditi prometnu signalizaciju ovisno o trenutnom prometu, raspodijeliti energiju pametnije i efikasnije i sl. 5G će omogućiti primjenu novih aplikacija i poslovnih modela poput virtualne stvarnosti, automatiziranih vozila, naprednih rješenja u industriji i poljoprivredi, području javne sigurnosti, financijskih usluga, zdravstva te energetike.

Posljedica velike primjene 5G mreže je ovisnost njenih korisnika o ispravnom funkcioniranju mreže kao i zaštiti velike količine podataka koja će prolaziti kroz njih. Sigurnost 5G mreže velikim dijelom ovisi o opremi pomoću koje se realizira. Od dobavljača opreme, mobilnih operatora (dalje u tekstu: operatori) i drugih sudionika se očekuje sudjelovanje u procesima planiranja, razvoja, testiranja, implementacije i održavanja opreme te je važno da su sigurnosni aspekti uključeni u sve procese.

Dobavljači za koje se sumnja da imaju implementirana stražnja vrata na opremi za pristup i krađu podataka te čijim poslovanjem upravlja država smatraju se visokorizičnima. Velik broj zemalja nastoji smanjiti ili potpuno zabraniti uporabu opreme takvih dobavljača. Australija, Indija, Japan i SAD su zabranili 5G opremu kineskih tvrtki Huawei i ZTE za koje tvrde da predstavljaju rizik za njihovu nacionalnu sigurnost [1]. S druge strane, osnivač Huaweija, Ren Zhengfei je u intervju za BBC 25. veljače 2019. izjavio da je kineska vlada jasno naglasila kako neće od tvrtki tražiti instalaciju stražnjih vrata niti će to činiti Huawei. Prije će zatvoriti tvrtku [2].

I u državama članicama Europske Unije (EU) se provode konkretne radnje kako bi se uskladio pristup sigurnosti 5G mreža pa je tako od svake članice zahtijevana provedba nacionalne procjene rizika 5G mrežne infrastrukture. Cilj procjene jest prepoznati najvažnije prijetnje i aktere koji ih uzrokuju, najosjetljiviju infrastrukturu i glavne slabosti (uključujući tehničke i druge vrste slabosti) koje utječu na 5G mreže. Na temelju procijenjenih rizika objavljen je EU Toolbox s nizom mjera za ublažavanje procijenjenih rizika [3] te se od svake članice zahtijeva usklađivanje postojećih zakona o sigurnosti mobilnih mreža i usluga s mjerama koje pojedina članica smatra prikladnim za ublažavanje rizika.

Zastupnici Europskog parlamenta iz pet različitih političkih grupa izrazili su zabrinutost zbog visokorizičnih dobavljača opreme te su 14. listopada 2020. uputili pismo Europskoj komisiji. Od Europske komisije i država članica EU-a traže intenzivniju provedbu mjera iz Toolbox-a, provođenje zajedničke procjene i kategorizacije visokorizičnih dobavljača kao i prestanak financiranja korištenja tehnologije visokorizičnih dobavljača telekomunikacijske opreme europskim sredstvima tj. novcem poreznih obveznika. Nadalje predlažu zatvaranje europskog tržišta javne nabave za tvrtke iz onih trećih zemalja koje europskim tvrtkama ograničavaju pristup vlastitim tržištima nabave te smanjenje pristupa tržištu tvrtki iz trećih zemalja koje su dobile značajnu državnu potporu od svojih matičnih država, osobito ako im to omogućuje dominaciju na globalnom tržištu na štetu poštene konkurencije i europskih dobavljača opreme. U pismu se navodi kako su najrelevantniji dobavljači 5G-a na globalnoj razini europski Ericsson i Nokia te kineski Huawei i ZTE. Kao i sve kineske tvrtke, i Huawei i ZTE su prema kineskom zakonu dužne poštivati

kineski nedemokratski autoritarni režim što uključuje korištenje mreža za kontrolu vlastitog stanovništva i špijuniranje zapadnih vlada, tvrtki i građana. Te dobavljače smatraju visokorizičnima i njihova bi tehnologija u europskim 5G mrežama predstavljala sigurnosnu prijetnju. Također navode kako postoji izražen nedostatak reciprociteta između EU-a i Kine u pristupu tržištu 5G dobavljača. Dok je tržište EU-a otvoreno za kineske dobavljače, Kina je gotovo u potpunosti zatvorila svoje tržište za europske dobavljače, unatoč suprotnom obećanju. U prvoj polovici 2020., na prvim velikim 5G natječajima koji uključuju prodaju i implementaciju stotina tisuća mobilnih baznih stanica diljem Kine, kineskim je dobavljačima dodijeljen tržišni udio od gotovo 90% [4].

Cilj rada je ukazati na utjecaj dobavljača opreme na očuvanje sigurnosti i privatnosti podataka koji se prenose, obrađuju i pohranjuju u 5G mreži. Istaknuti su dobavljači opreme iz Kine zbog tamošnjih zakona kojima zemlja može upravljati dobavljačima i ugroziti sigurnost 5G opreme i usluga. Prilikom odabira dobavljača operatori bi trebali slijediti mjere iz EU Toolboxa, procijeniti profil rizika dobavljača i primijeniti ograničenja na visokorizične dobavljače.

Rad je strukturiran na sljedeći način: u drugom poglavlju opisane su karakteristike i arhitektura 5G mreže. U trećem poglavlju su opisani sigurnosni aspekti i sigurnosne domene 5G mreže. U četvrtom poglavlju su navedeni i uspoređeni vodeći dobavljači 5G opreme. U petom poglavlju su opisani otkriveni slučajevi prisluškivanja i krađe podataka uzrokovanih malicioznim radnjama nad mrežnom opremom tvrtki Ericsson i Huawei te krađa intelektualnog vlasništva tvrtke Nortel. U šestom poglavlju je izdvojena kineska legislativa, opisane ranjivosti, prijetnje i rizici od kineske opreme te mjere za ublažavanje rizika. Napori EU-a u očuvanju povjerljivosti, cjelovitosti i dostupnosti 5G mreža i usluga opisani su u sedmom poglavlju. Osmo poglavlje donosi zaključak rada.

2. Karakteristike i arhitektura 5G mreže

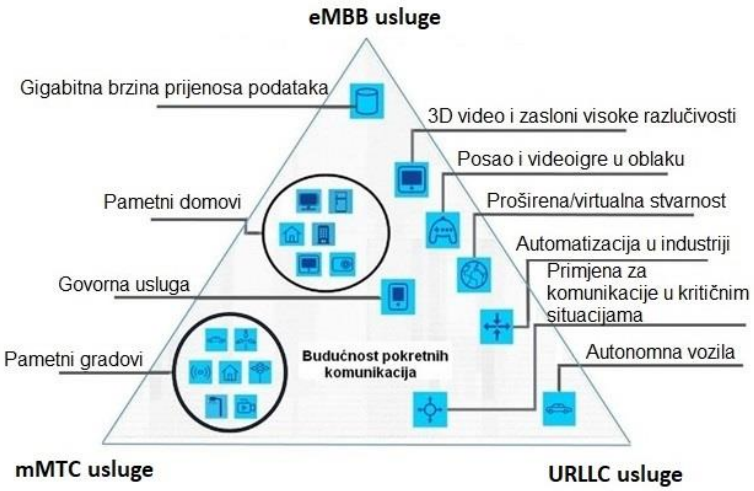
Razvoj generacija mobilnih mreža započeo je 1980-ih, od prve do današnje pete. U tom razdoblju svjedočili smo uvođenju govorne usluge u pokretu, usluge slanja/primanja tekstualnih poruka, mobilnih podatkovnih usluga vrlo malih brzina prijenosa do onih današnjih koje omogućuju prijenos videa visoke razlučivosti u stvarnom vremenu.

U nastavku su opisane karakteristike i arhitektura 5G mreže.

2.1 Karakteristike 5G mreže

5G telekomunikacijske tehnologije trebaju ispuniti tri osnovna zahtjeva: veliku propusnost, malo kašnjenje i veliku gustoću spojenih uređaja te pružiti nove vrste usluga: usluge naprednog mobilnog širokopojasnog pristupa (engl. *Enhanced Mobile Broadband*, eMBB), usluge visoke pouzdane komunikacije niskog kašnjenja (engl. *Ultra-Reliable and Low-Latency Communications*, URLLC) i usluge masivne komunikacije stroja sa strojem (engl. *massive Machine-Type Communications*, mMTC) [5].

eMBB usluge poput videa visoke razlučivosti (4K/8K), virtualne i proširene stvarnosti zahtijevaju veliku propusnost [5]. Pragovi definirani u zahtjevima Međunarodne telekomunikacijske unije (engl. *International Telecommunication Union*, ITU) za eMBB su postavljeni na najmanje 20 Gbps u preuzimanju i 10 Gbps u postavljanju. Što se tiče kašnjenja, URLLC usluge poput autonomne ili potpomognute vožnje, Interneta vozila i daljinskog upravljanja zahtijevaju malo kašnjenje, do 1ms [6]. S mMTC-om uslugama se omogućuju scenariji koji zahtijevaju velik broj spojenih mobilnih uređaja - $10^6/km^2$ [5]. URLLC, eMBB i mMTC usluge su prikazane na Slika 2.1.



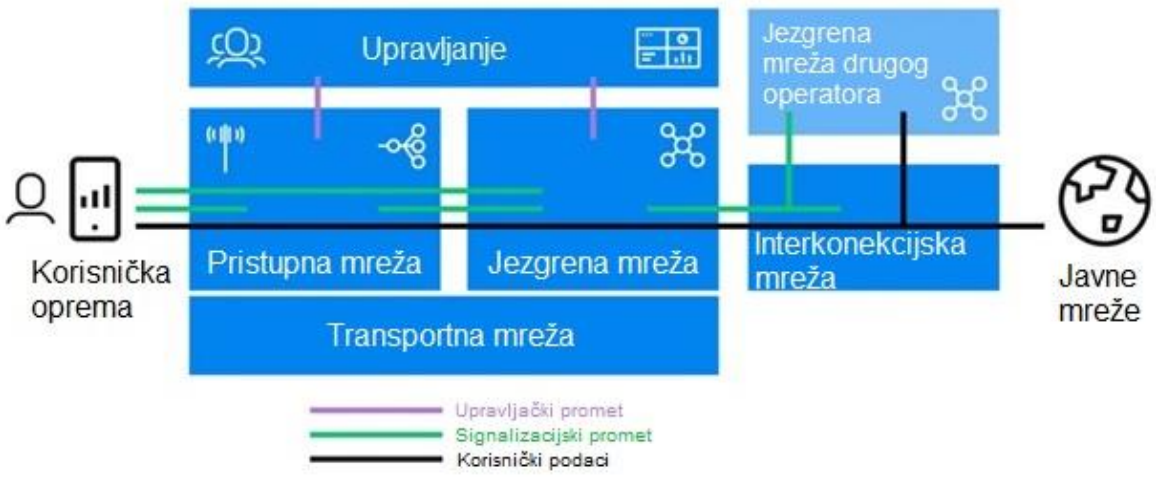
Slika 2.1 eMBB, URLLC i mMTC usluge [7]

Telekomunikacijske mobilne mreže su logički podijeljene na četiri segmenta: radio pristupnu mrežu (engl. *Radio Access Network*, RAN), jezgrenu mrežu, transportnu mrežu i interkonekcijsku mrežu [16]. RAN je instanca pristupne mreže i glavni dio modernih telekomunikacija. Nekoliko je vrsti pristupnih mreža poput *3rd Generation Partnership Project* (3GPP) pristupnih mreža: *Global System for Mobile Communications/General Packet Radio Service* (GSM/GPRS), *Universal Mobile Telecommunications System* (UMTS), *Evolved Universal Terrestrial Radio Access Network* (EUTRAN), *Next Generation RAN* (NG RAN tj. 5G). Jezgrena mreža pruža više usluga pretplatnicima koji su spojeni putem pristupne mreže na jezgrenu, npr. telefonske pozive i podatkovne veze. Transportna mreža povezuje pristupnu s jezgrenom mrežom te bazne stanice unutar radio pristupne mreže. Interkonekcijska mreža spaja različite jezgrene mreže [8].

Pojedina je mreža još dodatno podijeljena na signalizacijsku ravninu (engl. *control plane*) koja prenosi signalizacijski promet, korisničku ravninu koja prenosi korisničke podatke te ravninu upravljanja koja prenosi administrativni promet (Slika 2.2) [8].

Svakoj ravnini prijete napadi s različitim ciljevima:

a) Signalizacijskoj - pristup informacijama poput zemljopisnog položaja pretplatnika. Izmjenom signalizacijskog prometa može se pokušati preusmjeriti poziv ili presresti SMS poruke žrtve radi prisluškivanja ili uskraćivanja usluge.
b) Korisničkoj - pristup stvarnim podacima koji se prenose za korisnika. Bez odgovarajućih sigurnosnih mjera bila bi ugrožena privatnost korisnika i povjerljivost podataka poduzeća ili vlade. Stoga je važno očuvati cjelovitost podataka koji se prenose ovom ravninom.
c) Upravljačkoj - pristup mrežnim resursima, rukovanje i ometanje mrežnog prometa i podataka. Ublažavanje rizika i prijetnji povezanih s upravljanjem mrežom zahtijeva provedbu sigurnosnih politika i sigurnosnih kontrola kao što su kontrola pristupa i nadzor sigurnosti [8].

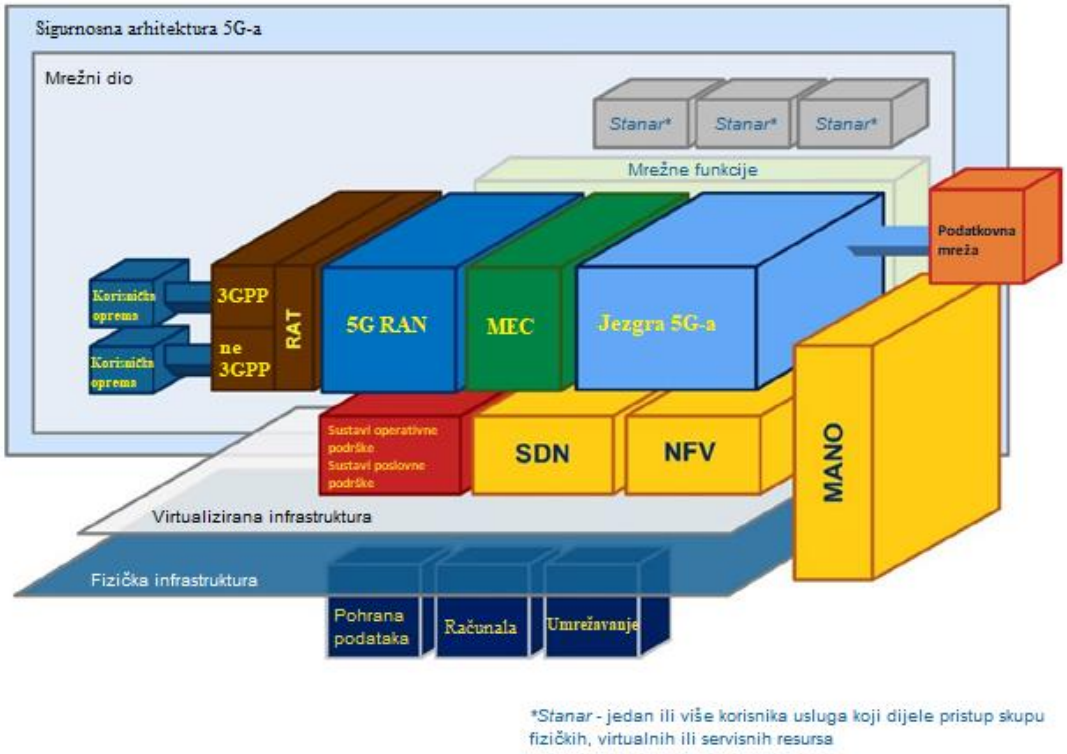


Slika 2.2 Mobilna komunikacijska mreža – logički elementi i logičke ravnine [8]

2.2 Arhitektura 5G mreže

Arhitektura 5G-a je projektirana na način da su podržani povezivanje i podatkovne usluge omogućujući tehnike kao što su virtualizacija mrežnih funkcija (engl. *Network Function Virtualization,* NFV), dijeljenje mrežnih reursa (engl. *Network Slicing*, NS) i softverski definirano umrežavanje (engl. *Software Defined Networking*, SDN) [6]. Na Slika 2.3 su prikazani dijelovi 5G mreže: fizička infrastruktura na kojoj je upogonjena virtualizacija mreže koja je podijeljena na dijelove, a svaki dio čini krajnji korisnički uređaj, RAN, jezgrena mreža, mrežne funkcije, nadzor i orkestracija mreže, podatkovni centri operatora, podatkovni centri u oblaku itd.

Svi ti dijelovi su objašnjeni u nastavku poglavlja.



Slika 2.3 Arhitektura 5G-a [6]

2.2.1 Fizička arhitektura 5G mreže

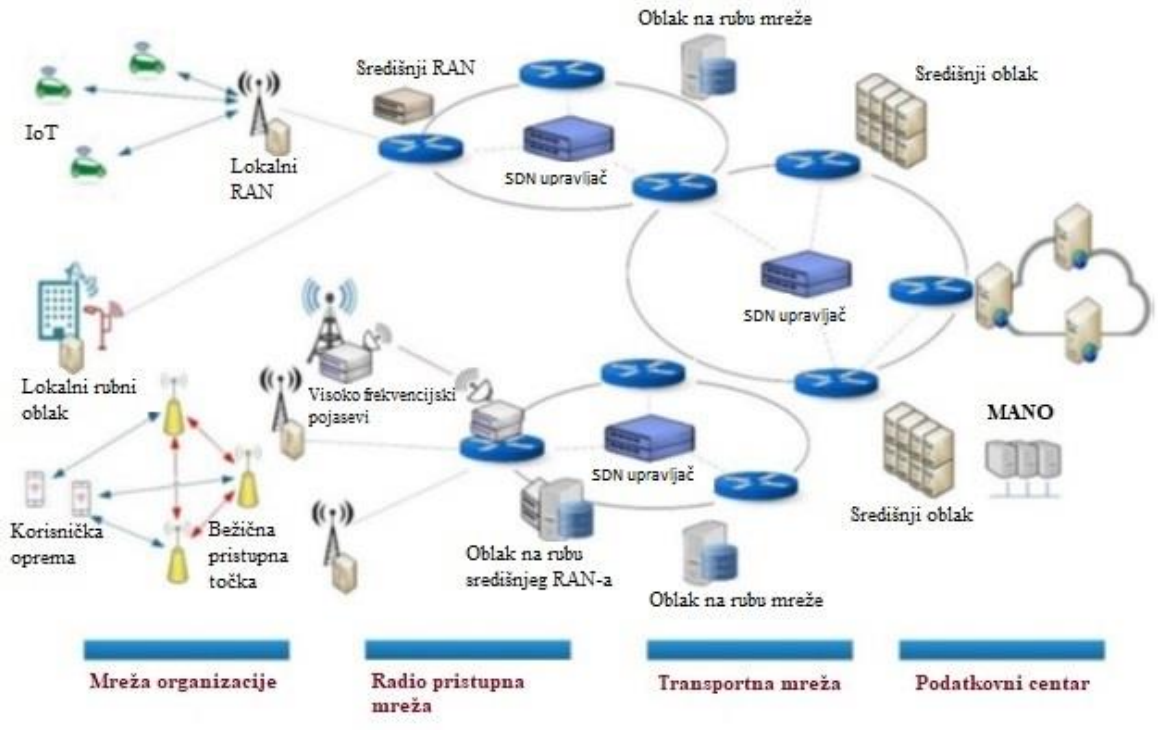
Jedan od najvažnijih aspekata pri prijelazu iz prethodnih generacija mobilnih telekomunikacija u 5G je virtualizacija i logička podjela mrežnih funkcija, bloka unutar mrežne infrastrukture s definiranim sučeljima i funkcionalnostima [9]. Mrežne funkcije su prethodno izvršavali mrežni uređaji koji su uglavnom bili namjenski (engl. *proprietary*) i nekompatibilni s

drugim rješenjima. Kod 5G-a mrežni softver može raditi na bilo kojem komercijalnom hardveru što operatore čini manje ovisnima o proizvođačima.

Ta značajna promjena omogućuje veliku skalabilnost, bržu implementaciju, manje troškove i integraciju različitih komponenti mreže. Zajednička fizička komponenta obavljat će više funkcija kao što su virtualne funkcije, dijeljenje mrežnih resursa itd. To u isto vrijeme povećava složenost implementacije softvera što je povezano s novim prijetnjama.

Unatoč tome, fizička 5G arhitektura i dalje će biti izložena općenitim prijetnjama poput: oštećenja, krađe, sabotaže, prirodnih katastrofa, ispada, kvarova i sl. Iako su u prijašnjim mobilnim mrežama takvi kvarovi imali više „ograničeni“ utjecaj u pružanju usluga, s virtualizacijom u 5G-u kvarovi fizičkih komponenti mogu imati pojačan utjecaj, posebno na zajedničke resurse. To povećava kritičnost komponenti fizičke infrastrukture 5G mreže jer će više usluga ovisiti o njima [6].

Oprema za fizičku mrežu prikazana je na Slika 2.4. Uključuje mrežni hardver, podatkovne centre operatora, podatkovne centre u oblaku, sve vrste korisničke opreme i hardver za radio pristup. Unatoč virtualiziranoj strukturi 5G mreže i svim uključenim mrežnim funkcijama, postojat će snažna ovisnost o fizičkoj infrastrukturi, osobito u početnoj fazi upogonjavanja 5G mreže koja će se velikim dijelom oslanjati na 4G mrežnu opremu [6].



Slika 2.4 Arhitektura 5G mreže [6]

2.2.2 Radio pristupna mreža

RAN je ključan dio 5G mreže jer omogućuje bežično povezivanje krajnjih uređaja s jezgrenom mrežom. Kroz vrijeme je evolurirao od raspodijeljenog RAN-a (engl. *Distributed RAN,* D-RAN), središnjeg RAN-a (engl. *Centralized RAN,* C-RAN) odnosno RAN-a u oblaku (engl. *Cloud* RAN), virtualnog RAN-a (engl. *Virtualized* RAN, vRAN) do otvorenog RAN-a (engl. *Open* RAN, O-RAN).

Kod D-RAN-a baznu stanicu čine jedinica osnovnog pojasa BBU (engl. *Baseband Unit*, BBU) i jedna ili više radio relejnih jedinica (engl. *Remote Radio Unit*, RRU). BBU se nalazi na središnjoj lokaciji, a RRU na vanjskoj lokaciji, bliže anteni. RRU se povezuje s antenom s jedne strane i BBU-om s druge. RRU je s BBU povezana optičkim vlaknima. RRU pretvara analogni, radiofrekvencijski (RF) signal u digitalni i obratno te filtrira i pojačava RF signal. BBU upravlja cijelom baznom stanicom, uključujući rad/održavanje i obradu signalizacije. Svaka je bazna stanica povezana s jezgrenom mrežom putem *backhaul*-a odnosno transportne mreže [10]. Dijelovi D-RAN-a su prikazani na Slika 2.5.

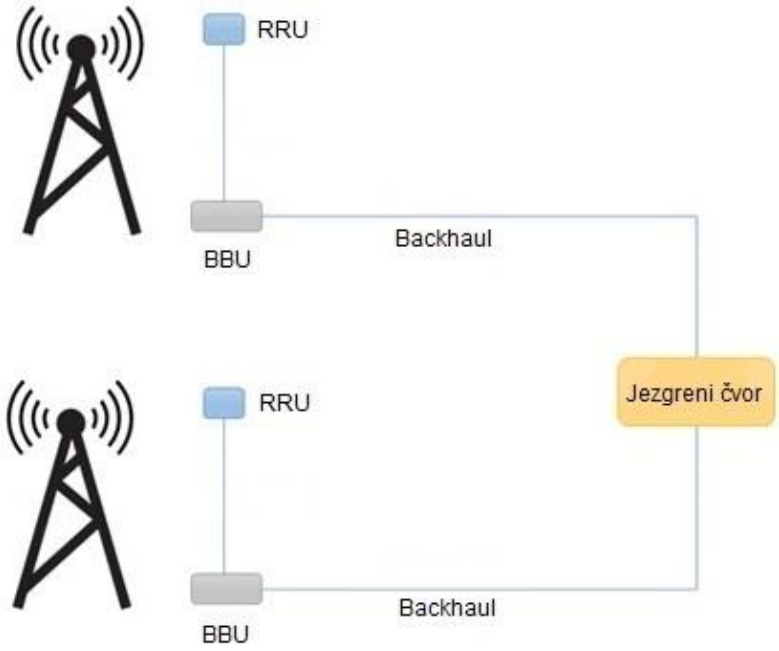
Kod C-RAN-a se BBU centralizira, a baznu stanicu čine RRU i antena. To rezultira novom vezom *fronthaul* između RRU-a i BBU-a. Prednost C-RAN-a uključuje smanjenje troškova implementacije i održavanja bazne stanice zbog centralizacije BBU-ova. Osim toga, poboljšava spektralnu učinkovitost i smanjuje smetnje između kanala jer centralizirani BBU-ovi mogu dinamički dijeliti resurse između više RRU-ova [10]. Dijelovi C-RAN-a su prikazani na Slika 2.6.

Daljnji razvoj C-RAN-a donosi podjelu BBU-a na središnju (engl. *Centralized Unit*, CU) i raspodijeljenu jedinicu (engl. *Distributed Unit*, DU). DU je odgovorna za fizički i podatkovni sloj, a CU za podatkovni i mrežni sloj referentnog modela povezivanja otvorenih sustava (engl. *Open System Interconnection Model*, OSI) [11]. CU se u ovom slučaju nalazi bliže jezgrenoj mreži što rezultira novom vezom *midhaul* između DU i CU [10]. Dijelovi C-RAN-a s podijeljenim BBU-om su prikazani na Slika 2.7.

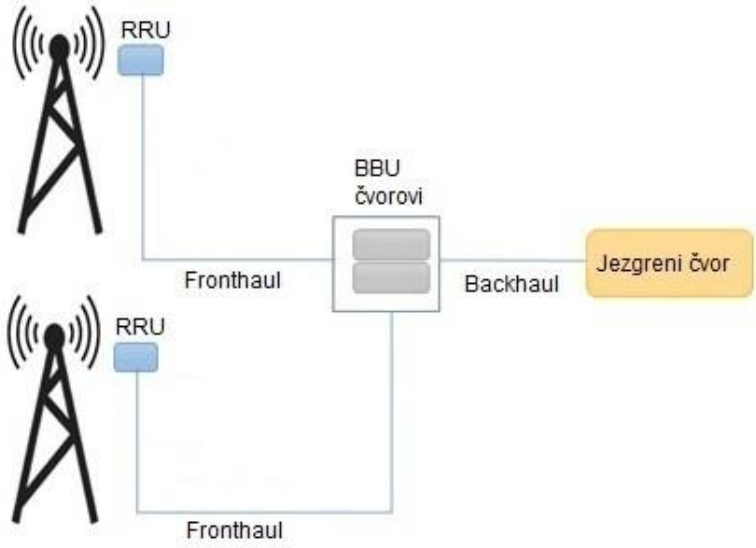
vRAN odvaja softver od hardvera virtualizacijom mrežnih funkcija čime se postiže skalabilnost, ušteda u hardveru i brza nadogradnja i zamjena aplikacija. vRAN koristi tehnologije virtualizacije za upogonjavanje CU-a i DU-a ili virtualnog BBU-a na poslužitelju koji više ne mora biti namjenski [10]. Dijelovi vRAN-a su prikazani na Slika 2.8.

Razlika između vRAN-a i C-RAN-a je ta što C-RAN koristi namjenski hardver dok vRAN koristi mrežne funkcije na poslužiteljskoj platformi. vRAN je zapravo vrsta C-RAN-a [10].

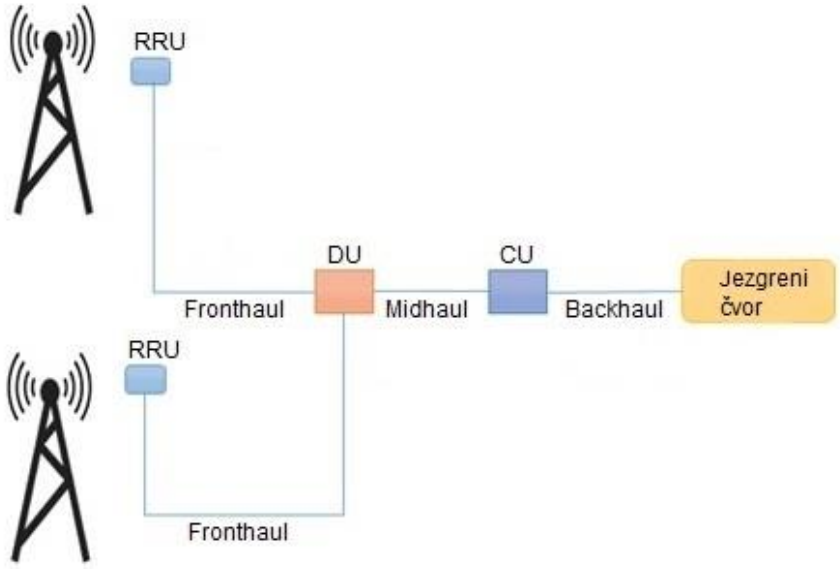
O-RAN predstavlja novu razinu vRAN-a. Kod vRAN-a se RRU, DU i CU moraju nabaviti od istog dobavljača. O-RAN za cilj ima otvoriti sučelja između RRU-a i DU-a kao i između DU-a i CU-a što znači da se te komponente mogu nabaviti od različitih dobavljača. Te otvorene komponente nazivaju se O-RU, O-DU i O-CU, modularni softveri koji se mogu podesiti na komercijalno dostupnom poslužiteljskom hardveru. Na Slika 2.9 su prikazani dijelovi O-RAN-a.



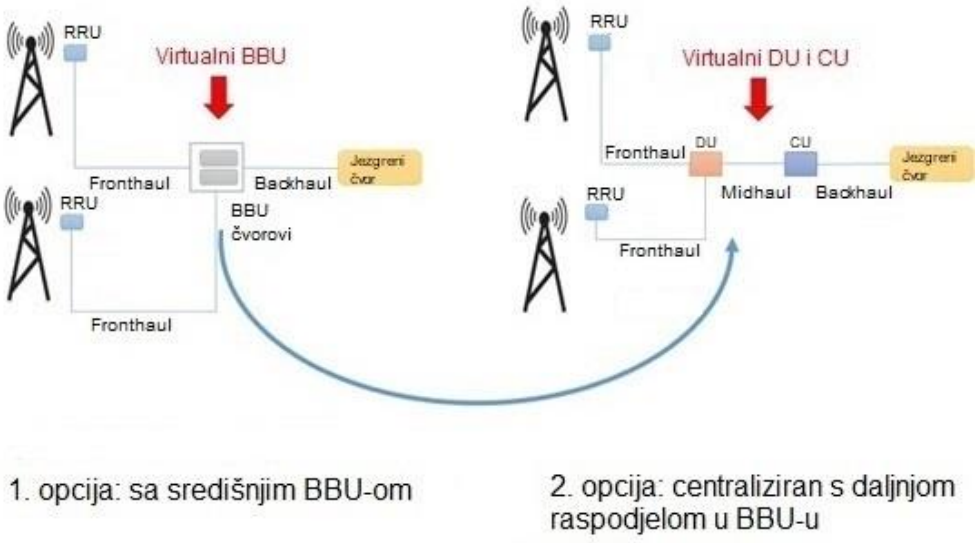
Slika 2.5 D-RAN [10]



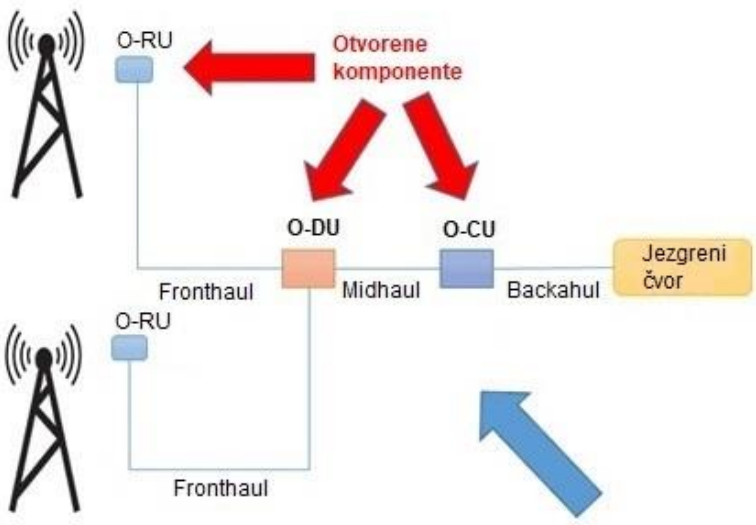
Slika 2.6 C-RAN [10]



Slika 2.7 C-RAN s podijeljenim BBU-om [10]



Slika 2.8 vRAN [10]



Slika 2.9 O-RAN [10]

2.2.3 Jezgrena mreža

Jezgrena mreža je središnji dio 5G infrastrukture. Glavna joj je svrha mobilnim pretplatnicima pružiti uslugu pristupa Internetu. Funkcije u jezgrenoj mreži su podijeljene na one u signalizacijskoj i korisničkoj ravnini [12].

Funkcije u signalizacijskoj ravnini su:

- Funkcija upravljanja pristupom jezgrenoj mreži i mobilnošću: upravljanje povezivanjem i dostupnošću, upravljanje mobilnošću, autentifikacija i autorizacija pristupa te usluge lociranja.
- Funkcija upravljanja korisničkim sjednicama: upravljanje svakom sjednicom krajnje korisničke opreme, uključujući dodjelu IP adrese, kontrolne aspekte kvalitete usluge itd.
- Funkcija kontrole politike: upravljanje politikama koje primjenjuju druge funkcije signalizacijske ravnine.
- Upravljanje korisničkim podacima: upravljanje identitetom korisnika, uključujući generiranje vjerodajnica za autentifikaciju.
- Funkcija autentifikacijskog poslužitelja: poslužitelj za autentifikaciju.
- Mrežna funkcija za pohranu strukturiranih podataka: "pomoćna" usluga za pohranu strukturiranih podataka. Može se implementirati pomoću SQL baze podataka u sustavu temeljenom na mikro uslugama.
- Mrežna funkcija za skladištenje nestrukturiranih podataka: "pomoćna" usluga za spremanje nestrukturiranih podataka. Može se implementirati pomoću *Key/Value Store*-a u sustavu temeljenom na mikro uslugama.

- Funkcija izloženosti mreže: sredstvo za izlaganje odabranih mogućnosti uslugama trećih strana, uključujući „prijevod“ između unutarnjih i vanjskih prikaza podataka. Može se implementirati putem poslužitelja programskog sučelja (engl. *Application Programming Interface*, API) u sustavu temeljenom na mikro uslugama.
- Funkcija mrežnog spremišta: sredstvo za otkrivanje dostupnih usluga. Može se implementirati pomoću *Discovery Service*-a u sustavu temeljenom na mikro uslugama.
- Funkcija odabira dijeljenja mrežnih resursa: sredstvo za odabir mrežnog dijela za pružanje određene usluge krajnjem korisniku [12].

Funkcija u korisničkoj ravnini: prosljeđivanje prometa između RAN-a i Interneta. Osim za prosljeđivanje paketa odgovorna je i za provođenje politika, zakonito presretanje, izvješćivanje o korištenju prometa i politiku kvalitete usluge [12].

U 5G-u je jezgrena mreža potpuno virtualizirana. SDN donosi pojednostavljeno upravljanje mrežom. NFV omogućuje tehnologiju za smještanje različitih mrežnih funkcija u različite mrežne komponente na temelju potreba/zahtjeva performansi te eliminira potrebu za hardverom specifičnim za funkciju ili uslugu [6].

2.2.4 Dijeljenje mrežnih resursa

Jedno od svojstava 5G mreže je dijeljenje mrežnih resursa, segmentacija jedne fizičke mreže na više jedinstvenih logičkih i virtualnih mreža, sukladno slučajevima korištenja. Primjerice, komunikacija između autonomnih automobila zahtijeva minimalno kašnjenje, ali ne nužno veliku propusnost dok je za slučaj korištenja proširene stvarnosti potrebna veća propusnost. 5G mreža prepoznaje manjak ili višak mrežnih resursa i ovisno o potrebi, dodaje ili oduzima resurse pojedinim uslugama čime se omogućuje njihov kontinuiran rad i kvaliteta usluga [6].

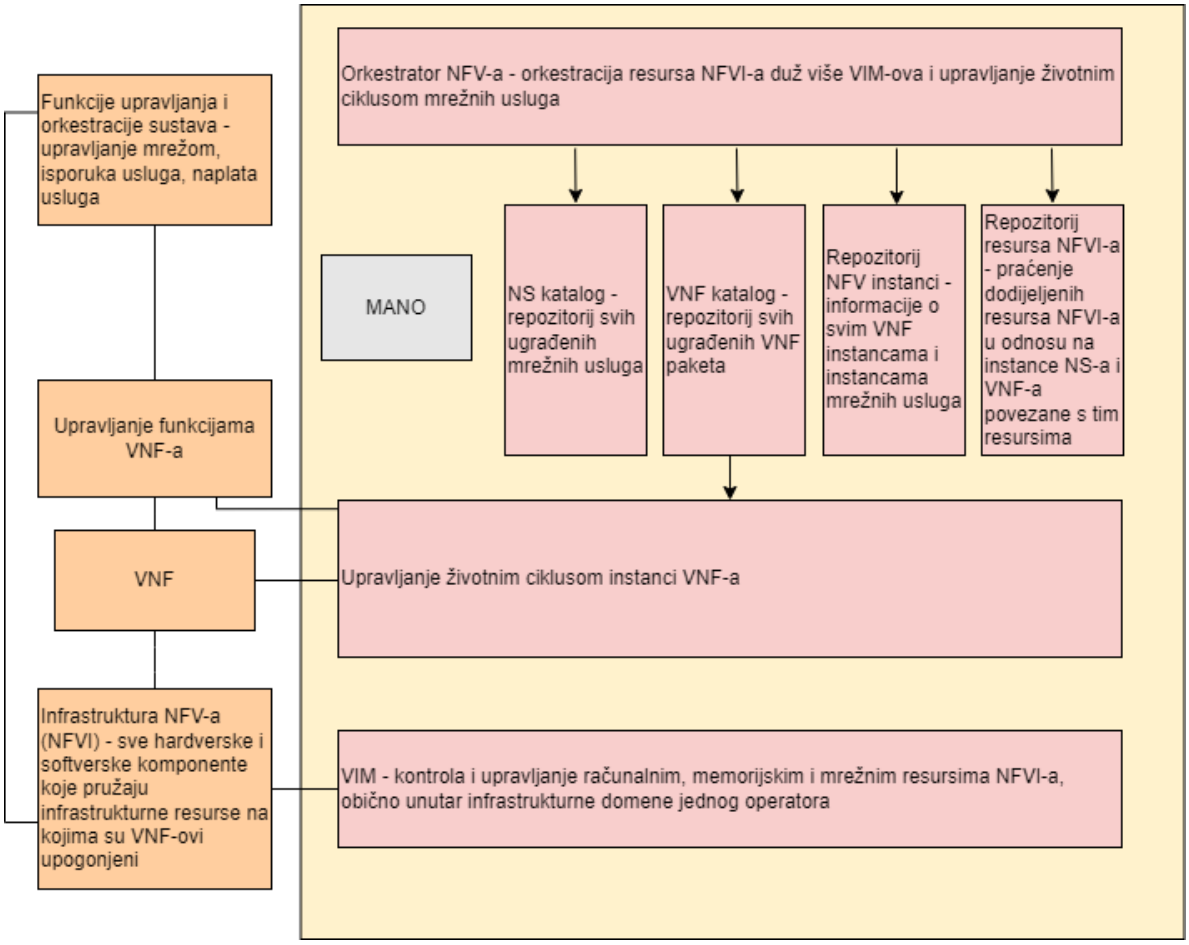
2.2.5 Upravljanje i orkestracija mreže

Upravljanje i orkestracija mreže (engl. *Management and Network Orchestrator*, MANO) jedna je od sigurnosno najkritičnijih komponenti 5G mrežne infrastrukture. Putem MANO-a se upravlja svim značajnim komponentama/funkcijama 5G-a, uključujući NFV, virtualiziranim mrežnim funkcijama (engl. *Virtualised Network Functions*, VNF) i virtualiziranom infrastrukturom (engl. *Virtualised Infrastructure Management*, VIM). MANO je podijeljen na tri funkcionalna bloka (Slika 2.10):

- orkestrator NFV-a - ugradnja novih mrežnih usluga (engl. *Network Service*, NS) i VNF paketa, upravljanje životnim ciklusom NS-a, upravljanje globalnim resursima, provjera valjanosti i autorizacija zahtjeva za resursima arhitekture NFV-a (engl. *NFV Infrastructure*, NFVI)
- upravljanje VNF-a - upravljanje životnim ciklusom instanci VNF-a

- upravljanje VIM-a - kontrola i upravljanje računalnim, memorijskim i mrežnim komponentama NFVI-a [13].

S obzirom na svoju važnu ulogu, za očekivati je da će MANO biti izložen brojnim napadima s potencijalno velikim utjecajem na cjelokupno upravljano 5G infrastrukturno okruženje [6].



Slika 2.10 Arhitektura MANO [6]

2.2.6 Virtualizacija mrežnih funkcija

Virtualizacijom mrežnih funkcija u 5G-u, poput dodjele IP adresa, mrežnog skaliranja, postavki vatrozida i sl. [14], smanjuje se ovisnost o namjenskoj mrežnoj opremi. NFV je arhitektura specifična za 5G kojom se funkcije mrežnih čvorova i fizičke mrežne funkcije zamjenjuju softverom koji se izvršava na virtualnim strojevima [15]. NFV uključuje i sigurnosne funkcije kao što su provjera autentičnosti i lociranje pretplatnika. Zbog osjetljivih podataka koje obrađuju, sigurnosne funkcije mogu biti izložene napadima s namjerom njihovog preuzimanja [6].

2.2.7 Softverski definirano umrežavanje

SDN omogućuje softversku dinamičku rekonfiguraciju topologije mreže čime se mreža može prilagoditi potrebama, npr. preusmjeravanje dostupnih kapaciteta prema zahtjevima (potrebi). SDN predstavlja mehanizam razdvajanja korisničke ravnine i ravnine upravljanja što omogućuje centralizirano upravljanje [14]. To razdvajanje ima dvije značajne posljedice:

a) smanjuje poteškoće u konfiguraciji i promjeni upravljačkih funkcija mreže jer ta funkcionalnost više nije odgovornost uređaja za prosljeđivanje u mreži koji imaju tendenciju vlasničke implementacije,
b) omogućuje dosljednu provedbu politika putem manjeg broja upravljača [6].

SDN nudi fleksibilnost u podešavanju usmjeravanja između dinamički konfiguriranih virtualiziranih mrežnih funkcija [8]. Dok SDN razdvaja, NFV se prvenstveno fokusira na optimizaciju samih mrežnih usluga virtualizacijom tih funkcionalnosti. Zbog svoje važne uloge u postavljanju i upravljanju virtualizirane 5G mreže, SDN se smatra ključnom komponentom za pružanje dostupnosti i cjelovitosti mrežnih funkcija [6].

2.2.8 Višepristupno rubno računarstvo

Višepristupno rubno računarstvo *(engl. Multi-access Edge Computing*, MEC) predstavlja uslugu računarstva u oblaku na rubu mreže, za korisničke aplikacije koje zahtijevaju visoke propusnosti i malo kašnjenje. MEC se nalazi u logičnoj blizini baznih stanica gdje putem ovlaštenih trećih strana pretplatnicima 5G mreže nudi mogućnosti obrade i pohrane podataka.

MEC poboljšava mobilno iskustvo korisnika pokrivanjem usluga koje su se u prethodnim generacijama mobilnih mreža izvršavale na uređaju krajnjeg korisnika. Kroz mogućnosti MEC-a, razne usluge mogu se konvergirati u jednu komponentu, kao što su usluge lokacije, video, virtualna stvarnost itd. Očekuje se da će MEC biti jedan od glavnih pokretača šire pokrivenosti i prodora 5G mreže [6].

3. Sigurnosna arhitektura 5G mreže

Sigurnost je kritičan aspekt svakog komunikacijskog sustava, a posebno mobilnih mreža. Bežičnu komunikaciju može presresti napadač s tehničkim znanjem i opremom za dekodiranje radio signala unutar određenog dometa bazne stanice zbog čega postoji rizik od prisluškivanja ili upravljanja prijenosom podataka. Nadalje, privatnost korisnika se može ugroziti lociranjem odnosno praćenjem kretanja korisnika između radio stanica u mreži.

Postoje i regulatorni zahtjevi koji se odnose na sigurnost i oni se mogu razlikovati između zemalja i regija. Takvi se propisi odnose na iznimne situacije u kojima relevantne agencije mogu zatražiti informacije o aktivnostima uređaja i korisnika, kao i presretati telekomunikacijski promet. Okvir u komunikacijskom sustavu koji to podržava zove se zakonito presretanje. Mogu postojati i propisi koji osiguravaju zaštitu privatnosti krajnjih korisnika kod uporabe mobilnih mreža. Zahtjevi poput ovih obuhvaćeni su nacionalnim i/ili regionalnim zakonima i propisima od strane odgovornih vlasti za određenu državu ili regiju. Sukladno tome, 5G mora omogućiti potrebne sigurnosne značajke kako bi se ispunili regulatorni zahtjevi [16].

U nastavku su opisani različiti sigurnosni aspekti u mobilnim mrežama, sigurnosni aspekti koji se odnose na krajnje korisnike, sigurnosni aspekti unutar i između mrežnih entiteta te ključni sigurnosni koncepti i sigurnosne domene. Fokus je na standardima definiranim u 3GPP-u [17]. Poglavlje se zaključuje procesom dobivanja uvjerenja o sigurnosti mrežne opreme.

3.1 Sigurnosni zahtjevi

Prilikom projektiranja sustava 5G, 3GPP se složio oko cjelokupnih sigurnosnih zahtjeva za 5G standard. To uključuje zahtjeve sustava za npr. autentifikaciju i autorizaciju pretplatnika, kriptiranje i zaštitu cjelovitosti između korisničke opreme i mreže itd. Postoje i sigurnosni zahtjevi za svaki entitet kao što su korisnička oprema, bazna stanica i sl. što uključuje zahtjeve za sigurnu pohranu i obradu pretplatničkih vjerodajnica i ključeva, podršku za određene algoritme kriptiranja, zaštitu cjelovitosti itd. [16]. Neki od sigurnosnih zahtjeva su opisani u nastavku.

3.2 Sigurnosne usluge

Prije no što se korisniku odobri pristup mreži, mora se provesti autentifikacija, uz iznimke za regulatorne usluge poput hitnih poziva što ovisi o lokalnim propisima. Tijekom autentifikacije korisnik dokazuje da je onaj za koga tvrdi da jest. Kod 5G-a je potrebna međusobna autentifikacija: mreža autentificira korisnika, a korisnik autentificira mrežu. Autentifikacija se obično vrši na način kojim svaka strana dokazuje da ima pristup tajni koja je poznata samo sudjelujućim stranama, na primjer lozinci ili tajnom ključu [16].

Mreža također provjerava ima li korisnik pravo pristupa traženoj usluzi, na primjer 5G uslugama putem određene pristupne mreže. To znači da korisnik mora imati odgovarajuće privilegije odnosno pretplatu za tražene vrste usluga. Autorizacija za pristupnu mrežu odvija se često istovremeno s autentifikacijom. Također, mogu se zahtijevati različite vrste autorizacije u različitim dijelovima mreže i u različitim slučajevima, ovisno o vrsti usluge koju korisnik traži. Mreža može autorizirati uporabu određene pristupne tehnologije, određene podatkovne mreže, određen profil kvalitete usluge (engl. *Quality of Service*, QoS), određene brzine prijenosa, pristup određenim uslugama itd.

Po odobrenju pristupa, potrebno je zaštititi signalizacijski promet i korisničku ravninu između korisničke opreme i mreže te između različitih entiteta u mreži za što se mogu primijeniti kriptiranje i zaštita cjelovitosti. Kriptiranje i zaštita cjelovitosti imaju različite svrhe, a potreba za kriptiranjem i/ili zaštitom cjelovitosti razlikuje se ovisno o kojem se prometu radi. Kriptiranje osigurava čitljivost prenesenih podataka samo predviđenim primateljima. Da bi se to postiglo, promet se kriptira i postaje nečitljiv svima koji ga uspiju presresti, osim entitetima koji imaju pristup pripadajućim kriptografskim ključevima. S druge strane, zaštita cjelovitosti štiti promet od izmjena od strane napadača između pošiljatelja i primatelja. Za kriptiranje/dekriptiranje kao i zaštitu cjelovitosti, pošiljatelj i primatelj trebaju kriptografske ključeve. Oni bi trebali biti različiti za različite svrhe i različite pristupe. To se svojstvo zove razdvajanje ključeva i važan je aspekt sigurnosnog dizajna 5G-a.

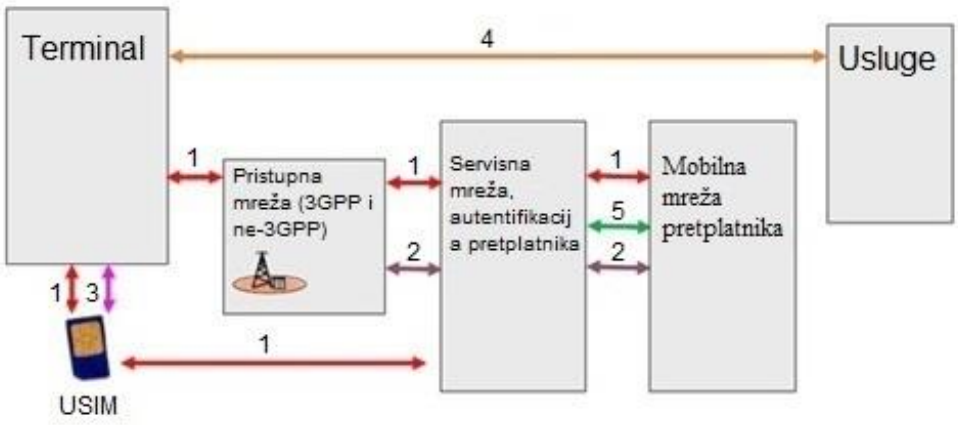
Zaštita privatnosti je još jedna važna sigurnosna značajka. Pod zaštitom privatnosti podrazumijevaju se značajke kojima se osigurava nedostupnost podataka o pretplatniku. Može uključivati mehanizme koji osiguravaju kriptiranje trajnog korisničkog identifikatora poslanog putem radio veze, u protivnom bi napadač mogao otkriti kretanje i obrasce kretanja korisnika [16].

3.3 Sigurnosne domene

3GPP TS 33.501 [18] dijeli sigurnosnu arhitekturu 5G-a na različite skupine ili domene, a svaka domena može imati svoj vlastiti skup sigurnosnih prijetnji i sigurnosnih rješenja:

1. Sigurnost mrežnog pristupa
2. Sigurnost mrežne domene
3. Sigurnost korisničke domene
4. Sigurnost aplikacijske domene
5. Sigurnost domene temeljene na uslugama
6. Vidljivost i konfigurabilnost sigurnosti.

Na Slika 3.1 prikazano je prvih pet sigurnosnih domena gdje je *Universal* SIM (USIM) funkcionalni ekvivalent SIM kartice. USIM je entitet koji pohranjuje informacije vezane za pretplatnika i implementira sigurnosne funkcije koje se odnose na autentifikaciju i kriptiranje na krajnjim korisničkim uređajima [19].



Slika 3.1 Pregled sigurnosne arhitekture 5G mreže [16]

3.3.1 Sigurnost mrežnog pristupa

Sigurnost mrežnog pristupa predstavlja skup sigurnosnih značajki koje korisniku pružaju siguran pristup mreži. To uključuje međusobnu autentifikaciju i značajke privatnosti, zaštitu signalizacijskog prometa i podataka korisničke ravnine. Ova zaštita može uključiti očuvanje povjerljivosti i/ili zaštite cjelovitosti podataka. Sigurnost mrežnog pristupa općenito ima specifične pristupne komponente – detaljna rješenja i algoritmi se razlikuju između pristupnih tehnologija. Napravljen je iskorak u učinkovitosti u pristupnim tehnologijama u 5G-u poput korištenja zajedničke pristupne autentifikacije. Moguća je autentifikacija putem mrežnog pristupnog servera i za 3GPP i ne-3GPP pristupne tehnologije [16]. Sigurnost mrežnog pristupa štiti i od napada na radio sučelja [20].

3.3.2 Sigurnost mrežne domene

Mobilne mreže sadrže brojne mrežne funkcije i referentne točke među njima. Sigurnost mrežne domene predstavlja skup sigurnosnih značajki koje ovim mrežnim funkcijama omogućuju sigurnu razmjenu podataka i zaštitu od napada na mreži između mrežnih funkcija [21]. Sigurnost mrežne domene definira sigurnosne značajke za sučelja između radio pristupne i jezgrene mreže te između kućne i uslužne mreže. Za sučelja između radio pristupne i jezgrene mreže mogu se koristiti posebni sigurnosni mehanizmi za zaštitu podataka kao što je protokol IPSec [20]. IPSec štiti IP promet i osigurava:

- Povjerljivost: kriptiranjem, podaci neće biti čitljivi nikome osim pošiljatelja i primatelja.
- Cjelovitost: izračunavanjem vrijednosti sažetka, pošiljatelj i primatelj će moći provjeriti da li je napravljena izmjena podataka u prijenosu.

- Autentifikaciju: međusobnom autentifikacijom pošiljatelja i primatelja osigurava se njihova međusobna komunikacija.
- *Anti-replay*: čak i ako su podaci kriptirani i autentificirani, napadač bi ih mogao pokušati presresti i ponovno ih poslati. Koristeći slijedne brojeve, IPSec neće prenijeti duple pakete [21].

3.3.3 Sigurnost korisničke domene

Sigurnost korisničke domene predstavlja skup sigurnosnih značajki koje osiguravaju fizički pristup mobilnom uređaju. Npr., korisnik će možda morati unijeti PIN za uporabu uređaja ili *Subscriber Identification Module* (SIM) kartice [16].

3.3.4 Sigurnost aplikacijske domene

Sigurnost aplikacijske domene predstavlja skup sigurnosnih značajki koje omogućuju aplikacijama u korisničkoj domeni i domeni pružatelja aplikacija sigurnu razmjenu podataka [20]. Protokol HTTPS (engl. *Hypertext Transfer Protocol Secure*) se koristi za sigurnu razmjenu podataka kod web pristupa, a okvir *IP Multimedia Subsystem* (IMS) se koristi za isporuku multimedijskih komunikacijskih usluga poput glasovnih, video te tekstualnih poruka putem IP mreže [22]. Sigurnosni mehanizmi aplikacijske domene transparentni su za cijelu mobilnu mrežu i pružaju ih pružatelji aplikacija [20].

3.3.5 Sigurnost domene temeljene na uslugama

Sigurnost domene temeljene na uslugama predstavlja skup sigurnosnih značajki koje omogućuju mrežnim funkcijama arhitekture zasnovane na uslugama (engl. *Service Based Architecture,* SBA) sigurnu komunikaciju s drugim mrežnim domenama kao i unutar domene poslužujuće mreže. Ove značajke uključuju sigurnosne aspekte registracije, otkrivanja i autorizacije mrežnih funkcija kao i zaštitu sučelja zasnovanih na uslugama. SBA čini osnovu jezgrene mreže 5G-a. Sigurnost ove domene je nova sigurnosna značajka u 5G mreži. Da bi se osigurala sigurnost između krajnje korisničke opreme u SBA-u, potrebni su sigurnosni mehanizmi poput sigurnosti transportnog sloja i otvorene autorizacije (engl. *Open Authorization*, OAuth) [20].

3.3.6 Vidljivost i konfigurabilnost sigurnosti

Vidljivost i konfigurabilnost sigurnosti predstavlja skup sigurnosnih značajki koje pružaju korisniku informaciju o operativnom statusu određene sigurnosne značajke [20]. U većini slučajeva

sigurnosne značajke su transparentne za korisnika i korisnik nije svjestan da su operativne. Za neke sigurnosne značajke korisnik bi trebao biti obaviješten o njihovom operativnom statusu. Npr., uporaba kriptiranja i zaštita cjelovitosti korisničkih podataka ovisi o konfiguraciji operatora te bi korisnik trebao imati informaciju koriste li se ili ne, primjerice, pomoću odgovarajućih simbola na zaslonu uređaja [16]. Konfigurabilnost sigurnosti pruža korisniku upravljanje sigurnosnim značajkama na krajnjem korisničkom uređaju poput pristupa USIM-u sa ili bez autentifikacije [23].

3.4 Uvjerenje o sigurnosti mrežne opreme

Uvjerenje o sigurnosti mrežne opreme (engl. *Network Equipment Security Assurance Scheme*, NESAS) definira sigurnosne zahtjeve i okvir procjene za siguran razvoj proizvoda i procese životnog ciklusa proizvoda te korištenje 3GPP definiranih sigurnosnih test slučajeva za sigurnosnu procjenu mrežne opreme. Sigurnosne zahtjeve i procese za NESAS je razvila GSMA u suradnji s 3GPP-om, operatorima i dobavljačima. NESAS omogućuje sigurnosnu osnovu za dokazivanje da proizvod zadovoljava listu sigurnosnih zahtjeva i da je razvijen u skladu s razvojem dobavljača i procesima životnog ciklusa proizvoda koji pružaju sigurnost [24].

Verzija NESAS-a, 2.0, će uključiti penetracijsko testiranje i verifikaciju kriptografskih mehanizama što prethodne dvije verzije, 1.0 i 1.1, nisu uključivale [28]. NESAS bi se trebao koristiti zajedno s drugim mehanizmima, posebno odgovarajućim skupom sigurnosnih politika koje pokrivaju cijeli životni ciklus mreže [24]. Revizori za sigurnost koje bira GSMA, tvrtke NCC Group i ATSEC [25], procjenjuju proces dok je drugi dio ocjene proizvoda vezan za laboratorijsko testiranje kako novih tako i nadograđenih proizvoda. Laboratoriji su ISO/IEC 17025 akreditirani.

Proces uključuje sljedeće korake:

a) dobavljači definiraju i primjenjuju sigurnosno projektiranje, razvoj, implementaciju i proces održavanja proizvoda,
b) dobavljači procjenjuju razinu usklađenosti proizvoda prema GSMA zahtjevima (engl. *Development i Product Lifecycle Security Requirements* [26]),
c) dobavljači demonstriraju te procese neovisnim revizorima za sigurnost koji procjenjuju usklađenost s GSMA sigurnosnim zahtjevima,
d) razine sigurnosti proizvoda se evaluiraju i dokumentiraju u testnim laboratorijima prema sigurnosnim zahtjevima definiranim unutar 3GPP *System Aspects* (SA3),
e) dokumentacija se šalje operatoru zajedno s kupljenim proizvodom [24].

SA3 definira zahtjeve i specifikaciju arhitektura i protokola za sigurnost i privatnost u 3GPP sustavima, dostupnost kriptografskih algoritama kao obavezni dio specifikacija, pruža zahtjeve i specifikacije za zakonito presretanje u 3GPP sustavima [27].

Procjene razvoja i životnog ciklusa proizvoda NESAS provodi prema sigurnosnim zahtjevima koji pokrivaju sljedeća područja:

- integrirana sigurnost,

- sustavi provjere inačica,
- praćenje promjena,
- pregled izvornog kôda,
- testiranje sigurnosti,
- edukacija osoblja,
- procesi otklanjanja ranjivosti,
- neovisnost u otklanjanju ranjivosti,
- upravljanje informacijskom sigurnošću,
- automatizirani proces stvaranja,
- kontrola okoline stvaranja,
- upravljanje podacima o ranjivostima,
- zaštita cjelovitosti softvera,
- jedinstveni identifikator izdanja softvera,
- komunikacija kod ispravljanja propusta,
- točnost dokumentacije,
- točka kontakta za sigurnost,
- upravljanje izvornim kôdom,
- kontinuirano poboljšanje,
- dokumentacija o sigurnosti [24].

Dobavljačima opreme NESAS donosi sljedeće prednosti:

- pruža akreditaciju od vodećeg svjetskog predstavničkog tijela mobilne industrije,
- donosi vrhunski sigurnosni pregled procesa povezanih sa sigurnošću,
- nudi jedinstven pristup sigurnosnim revizijama,
- izbjegava fragmentaciju i potencijalno oprečne zahtjeve za osiguranje sigurnosti na različitim tržištima [20].

Operatorima NESAS donosi sljedeće prednosti:

- postavlja strogi sigurnosni standard koji zahtijeva visoku razinu predanosti dobavljača,
- nudi „bezbrižnost“ budući su dobavljači primijenili odgovarajuće sigurnosne mjere i prakse,
- nema trošenja novca ni vremena na provođenje pojedinačnih revizija dobavljača [20].

Upravljanje NESAS-om bit će prepušteno Europskoj komisiji budući se ona mora pobrinuti za standard jer je GSMA komercijalna organizacija koja ne može, prema Zakonu o kibernetičkoj sigurnosti, akreditirati laboratorije i tijela za ovjeru. Samo će na taj način NESAS postati paneuropski standard prepoznat na razini vlade [28].

Tvrtke Ericsson, Nokia i Huawei su prošle NESAS-ovu procjenu i neovisnu reviziju razvoja i procesa životnog ciklusa dijela svojih 5G mrežnih proizvoda kako bi dokazale da je sigurnost integrirana u njihove procese projektiranja, razvoja, implementacije i održavanja opreme [29].

4. Vodeći dobavljači 5G opreme

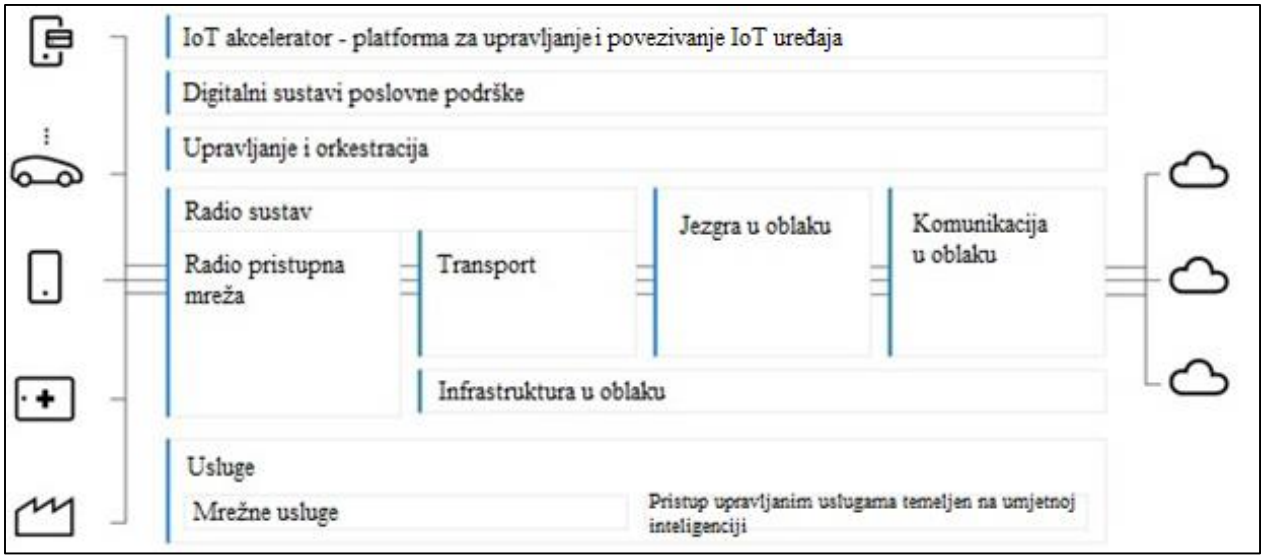
Gartnerovo istraživanje iz veljače 2022. [30] izdvaja 10 glavnih dobavljača mrežne opreme za 5G mrežnu infrastrukturu: Ericsson, FiberHome Telecommunication Technologies, Fujitsu, Huawei, Mavenir, NEC, Nokia, Rakuten Symhony, Samsung i ZTE. U ovom radu su izdvojeni vodeći, iz gornjeg desnog kvadranta: Ericsson, Nokia i Huawei (Slika 4.1) [31].

Slika 4.1 Čarobni kvadrant za dobavljače opreme za 5G mrežnu infrastrukturu [31]

4.1 Ericsson

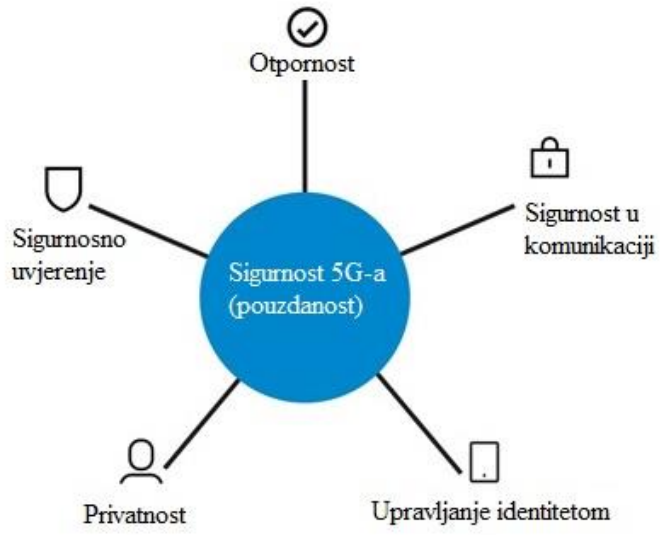
Ericsson je jedna od vodećih svjetskih tvrtki za informacijsku i komunikacijsku tehnologiju sa sjedištem u Stochkolmu u Švedskoj i podružnicama diljem svijeta [32]. S Nokijom i Huaweijem je vodeći svjetski proizvođač 5G opreme, a proizvode ju u Europi (Tallin, Estonija), Aziji (Nanjing, Kina) [33] i Americi (Sao Jose dos Campos, Brazil [34] i Lewisville, Texas [35]). Na Slika 4.2 je prikazana njihova 5G platforma. Pružaju usluge koje se temelje na umjetnoj inteligenciji i

automatizaciji. Radio sustav tvrtke Ericsson obuhvaća hardver, softver i vezane usluge za izgradnju modularnih i skalabilnih radio pristupnih mreža. Infrastruktura u oblaku obuhvaća NFV infrastrukturu. Nude jezgreni dio mreže u oblaku, a komunikacija u oblaku omogućuje komunikacijske usluge kao što su poruke, govor i video. Nude rješenja za upravljanje i orkestraciju mreže, naplatu usluga u stvarnom vremenu i platformu za povezivanje i upravljanje IoT uređajima.



Slika 4.2 5G platforma tvrtke Ericsson [36]

Pouzdanost 5G sustava Ericsson temelji na pet svojstava prikazanih na Slika 4.3: otpornost, sigurnost u komunikaciji, upravljanje identitetom, privatnost i sigurnosno uvjerenje (engl. *security assurance*) [37].



Slika 4.3 Pet svojstava koje doprinose pouzdanosti 5G sustava tvrtke Ericsson [37]

Otpornost na kvarove i napade u pristupnoj mreži se može postići razdvajanjem bazne stanice na dvije jedinice, središnju i raspodijeljenu. Ova podjela također olakšava prilagodbu u postavljanju sigurnosno osjetljivih funkcija pristupa 5G mreži na sigurnom središnjem mjestu, poput kriptiranja korisničke ravnine, dok se funkcije koje nisu osjetljive na sigurnost čuvaju na manje sigurnim raspodijeljenim lokacijama. U jezgrenoj mreži se grupe mrežnih funkcija odvajaju od drugih funkcija uz pomoć dijeljenja mrežnih resursa čime se određeni promet može prioritizirati.

Otpornost 5G usluga omogućuju i SBA funkcije koje koriste tehnologije zasnovane na softveru i oblaku. One se lako mogu skalirati ovisno o prometnom opterećenju, a mogu se i neovisno zamijeniti, ponovno pokrenuti ili izolirati u slučaju kvara ili napada [37].

5G sustav štiti podatke od prisluškivanja i izmjena čime se osigurava sigurnost u komunikaciji. Signalizacijski je promet kriptiran i zaštićen od izmjena. Promet korisničke ravnine je kriptiran te mu je moguće zaštiti cjelovitost. Glavna funkcija izvođenja ključeva temelji se na sigurnom algoritmu *Hash-based Message Authentication Code-Secure Hash Algorithm* (HMAC-SHA-256). Osim naslijeđenih sigurnosnih značajki 4G mreže, 5G uvodi nove sigurnosne značajke poput automatskog oporavka od zlonamjernih neusklađenosti sigurnosnih algoritama, odvajanja sigurnosnih ključeva između funkcija jezgrene mreže i brze sinkronizacije sigurnosnih konteksta u pristupnim i jezgrenim mrežama.

Upravljanje identitetom uključuje identifikaciju i provjeru autentičnosti pretplatnika izvan ili unutar roaminga čime se samo pretplatnicima osigurava pristup mrežnim uslugama. Sustav se temelji na skupovima snažnih kriptografskih algoritama i funkcijama generiranja ključeva te međusobnoj provjeri autentičnosti između uređaja i mreže. Jedna od najvrjednijih novih sigurnosnih značajki u 5G sustavu je novi okvir za provjeru autentičnosti kojim operatori mogu fleksibilno birati vjerodajnice za provjeru autentičnosti, formate identifikatora i metode provjere autentičnosti za pretplatnike i IoT uređaje. Prethodne generacije mobilnih mreža zahtijevale su

fizičke SIM kartice dok 5G sustav dopušta i druge vrste vjerodajnica poput certifikata, dijeljenih tajni i tokena (engl. *token cards*). Još jedna vrijedna nova sigurnosna značajka je mogućnost uvida operatora u prisutnost pretplatnika tijekom postupka autentifikacije, čak i u roamingu. To ublažava potencijalne prijevare te štiti od napada na sigurnost i privatnost pretplatnika ili operatora [37].

Privatnost se odnosi na zaštitu podataka pretplatnika koje neovlaštene strane mogu zlorabiti. Stupanjem odredbi i zakona o zaštiti osobnih podataka u Europi, poput GDPR-a (engl. *General Data Protection Regulation*), rješavanje pitanja privatnosti je postalo prioritetno u 5G mreži te je privatnost pretplatnika uključena u projektiranje opreme i usluga.

Podatkovni promet, telefonski pozivi, internetski promet i tekstualne poruke zaštićeni su najsuvremenijim kriptiranjem (engl. *state of the art*). Uređaji i mreža međusobno se autentificiraju i koriste signalizaciju kojom je zaštićena cjelovitost što neovlaštenoj strani onemogućuje dekriptiranje i čitanje prenesenih informacija.

5G sustav također može otkriti lažne bazne stanice. Iz podataka u izvješćima o prikupljenim mjerenjima s uređaja može se otkriti prisutnost lažnih baznih stanica koje pokušavaju dohvatiti podatke pretplatnika. Na primjer, kada jačina primljenog signala bazne stanice nije u skladu s očekivanom jačinom signala na određenom mjestu, prijavljena bazna stanica je vjerojatno lažna. Nakon otkrivanja prijetnji i malicioznih radnji izvršavaju se unaprijed postavljeni zadaci poput obavještavanja pretplatnika i kontaktiranja pravnih tijela [37].

Sigurnosno uvjerenje se izdaje za mrežnu opremu koja zadovoljava sigurnosne zahtjeve i implementirana je u skladu sa sigurnim razvojem i procesima životnog ciklusa proizvoda. Ovo je jamstvo posebno važno za mobilne sustave jer oni čine okosnicu povezanog društva te su u nekim jurisdikcijama klasificirani kao kritična infrastruktura.

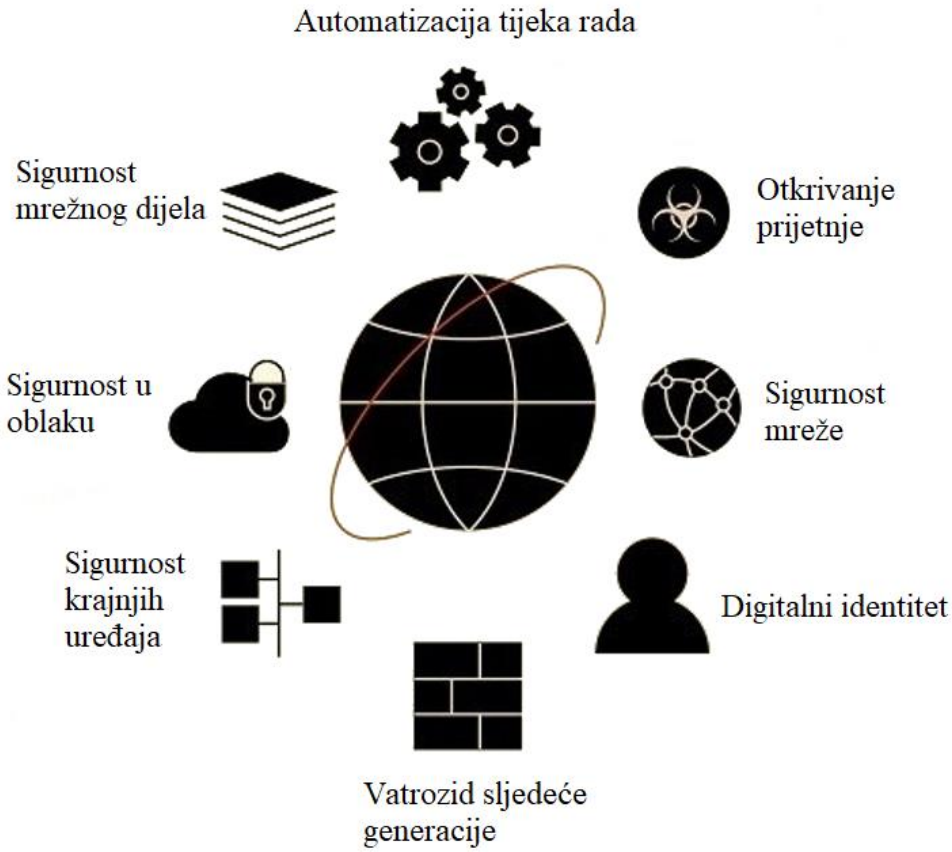
4.2 Nokia

Nokia Corporation (dalje u tekstu: Nokia) je finska multinacionalna tvrtka za telekomunikacije, informacijsku tehnologiju i potrošačku elektroniku sa sjedištem u Espoou u Finskoj. Tvrtka je osnovana 1865. i bila je vodeći proizvođač mobilnih uređaja na svijetu. Od 2018. je treći najveći svjetski proizvođač mrežne opreme [38]. S Ericssonom i Huaweijem vodeći je svjetski proizvođač 5G opreme, a proizvode ju u Finskoj (Oulu) [39] i Indiji (Chennai) [40].

Među njihovim 5G proizvodima izdvajaju se antene i bazne stanice u pristupnom dijelu mreže, mrežni usmjernici u transportnom dijelu mreže te otvorena i modularna jezgrena mreža izgrađena u oblaku [41].

Sigurnost 5G mreže treba biti omogućena s kraja na kraj, od uređaja, pristupne mreže do rubne mreže u oblaku i jezgrene mreže. To zahtijeva kombinaciju uvida, skalabilnosti i prilagodljivosti, tri svojstva koja u Nokiji zovu "trokut povjerenja" [42]. Nokijina sigurnosna rješenja prikazana na Slika 4.4 su:

- sigurnosne usluge s kraja na kraj: sigurnosna arhitektura i implementacija učinkovite sigurnosne kontrole za mreže s više dobavljača, više tehnologija i više generacija u stalnoj evoluciji,
- sigurnost krajnjih uređaja: zaštita od prijetnji od zloćudnih programa i mreže kompromitiranih računala,
- sigurnost IP mreže: zaštita od prijetnji na razini mreže samoobrambenom IP mrežnom infrastrukturom,
- otkrivanje i integracija: zaštita krajnjih uređaja, oblaka i mreža na temelju potpisa i anomalija [42],
- analiza i inteligencija: analiza prijetnji, korisnika, ponašanja entiteta radi povećanja vidljivosti i učinkovitosti,
- automatizacija i orkestracija: orkestracija automatiziranih procedura radi skraćivanja vremena odgovora na incident [43].



Slika 4.4 Nokijina sigurnosna rješenja [43]

Više od 7 bilijuna bežičnih uređaja koje koristi više od 7 milijardi ljudi bit će međusobno povezano uz pomoć 5G mreže što povećava broj sigurnosnih prijetnji i stvara veći fokus na privatnost [44]. Iz korisničke perspektive, ugroza privatnosti se odnosi na otkrivanje lokacije, identiteta i drugih osjetljivih podataka. Podaci o lokaciji korisnika se mogu otkriti ako se dozna s kojom antenom mobilni korisnik komunicira [44]. Identitet mobilnih pretplatnika je ugrožen napadima otkrivanja jedinstvenog broja svakog pretplatnika mobilne mreže (engl. *International Mobile Subscriber Identity*, IMSI). Ako se otkrije IMSI, napadač može presresti mobilni promet u određenom području i pratiti aktivnosti pretplatnika. Iako napadač može vidjeti broj odlaznih poziva ili tekstualnih poruka, ne može vidjeti sadržaj te poruke.

Prikupljanje podataka također može ugroziti privatnost korisnika 5G-a. Gotovo sve aplikacije za pametne telefone zahtijevaju osobne korisničke podatke prije ili tijekom instalacije. Programeri aplikacija rijetko spominju kako i gdje se ti podaci pohranjuju i za što će se koristiti. 5G mreže nemaju fizičkih granica i koriste pohranu podataka u oblaku. Posljedično, 5G operatori ne mogu zaštititi niti kontrolirati korisničke podatke pohranjene u oblaku. Budući svaka država ima različite razine mjera privatnosti i provedbe, privatnost korisnika ozbiljno je ugrožena ako i kada se podaci pohrane u oblak druge zemlje [44].

5G arhitektura treba uključiti pristup *security-by-design* koji je usmjeren na usluge i očuvanje privatnosti. Operatori trebaju usvojiti hibridni pristup temeljen na oblaku te osjetljive podatke pohraniti lokalno, a manje osjetljive u oblaku. To operatorima pruža bolji pristup i kontrolu nad podacima te mogu odlučiti gdje i s kim će ih podijeliti [44].

Privatnost temeljena na lokaciji zahtijeva tehnike i sustave temeljene na anonimnosti gdje se pravi identitet korisnika može sakriti, moguće pomoću pseudonima. Poruke bi također trebale biti kriptirane prije nego se pošalju pružatelju usluga koji se temelji na lokaciji. Obfuskacijske tehnike kojima se smanjuje kvaliteta informacija o lokaciji također se mogu koristiti za zaštitu privatnosti lokacije [44].

Kako bi se spriječili napadi otkrivanja IMSI broja, mobilni operatori mogu zaštititi identitet korisnika pomoću privremenog identiteta mobilnog pretplatnika (engl. *Temporary Mobile Subscriber Identity,* TMSI) koji se dodjeljuje svakom mobilnom uređaju i koji mreža mijenja u redovitim intervalima. To otežava identifikaciju mobilnih uređaja i sprječava identifikaciju pretplatnika i/ili prisluškivanje radio sučelja [44].

4.3 Huawei

Huawei Technologies Co., Ltd. (dalje u tekstu: Huawei) je kineska multinacionalna tvrtka koja proizvodi telekomunikacijsku opremu i potrošačku elektroniku. Sjedište tvrtke je u gradu Shenzhenu u pokrajini Guangdong u Kini [45]. S Ericssonom i Nokijom je vodeći svjetski proizvođač 5G opreme, a proizvode ju u Kini (Dongguan) [46] i od 2023. u Francuskoj (Brumath) [47]. Huawei proizvodi mrežnu opremu za sve dijelove 5G mreže: pristupnu, jezgrenu, transportnu kao i 5G usluge u oblaku. Huawei je vodeća telekomunikacijska tvrtka u području ulaganja u

istraživanje i razvoj: između 2009. i 2013. su uložili više od 600 milijuna američkih dolara u istraživanje 5G tehnologije, a 2017. i 2018. gotovo 1,4 milijarde američkih dolara u razvoj 5G proizvoda [48].

Huawei je privatna tvrtka u potpunom vlasništvu svojih zaposlenika. Nijedan vladin ured niti organizacija treće strane ne posjeduje dionice tvrtke, ne miješa se u njeno poslovanje niti utječe na donošenje odluka [49]. Ipak, sukladno Zakonu o tvrtkama Narodne Republike Kine u Huaweiju je oformljen komitet komunističke partije Kine za koji Huawei tvrdi da ne sudjeluje ni u kakvim operativnim ili poslovnim odlukama tvrtke [50]. Huawei je obavezan, bez ustupanja i iznimki, ustupiti potrebne podatke vlasti, obavještajnim agencijama te organima državne sigurnosti i prihvatiti nadzor vlade.

Svoj uspjeh Huawei temelji na usmjerenosti prema klijentu i realizaciji projekata što postiže brzim promjenama u organizaciji tvrtke. Zaposlenici u srednjem i višem menadžmentu se rotiraju na različitim poslovima unutar najviše tri godine, a nakon 45. godine starosti preporuka je posao nastaviti kod dobavljača Huawei proizvoda ili u edukacijskim organizacijama kako bi se njihovo iskustvo dalje prenosilo, dok njihovo mjesto zauzimaju mlađi zaposlenici. Ta superfluidna tvrtka zapošljava preko 170.000 osoba od kojih više od 40.000 nisu Kinezi [51].

Od 2018. kibernetička sigurnost i zaštita privatnosti su glavni prioriteti Huaweija [49]. Huawei se u svom istraživanju i razvoju snažno usredotočuje na sigurnost tijekom razvoja proizvoda pridržavajući se načela *security by design* i *security in process*.

2010. je Huawei počeo ugrađivati aktivnosti kibernetičke zaštite u proces razvoja svojih proizvoda prema industrijskim sigurnosnim praksama i standardima, poput *Open Web Application Security Project* (OWASP) modela zrelosti *Software Assurance Maturity Model* (OpenSAMM), *Building Security In Maturity Model* (BSIMM), *Microsoft Security Development Lifecycle* (SDL) i Okvira za kibernetičku sigurnost Nacionalnog instituta za standarde i tehnologiju (engl. *The National Institute of Standards and Technology Cybersecurity Framework*, NIST CSF) kao i zahtjevima korisnika i vlada za kibernetičku sigurnost. Te aktivnosti uključuju sigurnosne zahtjeve, projektiranje, razvoj, testiranje, objavljivanje i upravljanje ranjivostima. Kontrolne točke se u tom procesu koriste kako bi se osiguralo učinkovito provođenje sigurnosnih aktivnosti u razvoju proizvoda i rješenja. Ova praksa poboljšava robusnost proizvoda i rješenja, poboljšava zaštitu privatnosti i osigurava sigurne proizvode i rješenja [20].

Huawei je u fazi projektiranja proizvoda proširio model prijetnje lažiranjem, krivotvorenjem, opovrgavanjem, otkrivanjem informacija, uskraćivanja usluge i povećanjem privilegija (engl. *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege*, STRIDE) sa stablom napada i procjenom utjecaja na privatnost nazvavši ga naprednim STRIDE-om (engl. *Advanced* STRIDE, ASTRIDE). Huawei je također razvio standarde sigurnog dizajna kako bi inženjere usmjerio u sigurni dizajn, pozivajući se na najbolje prakse u industriji [20].

U fazi razvoja proizvoda Huawei je razvio vlastite standarde sigurnog kodiranja koji se pozivaju na najbolju praksu industrijskih standarda za sigurno kodiranje: *Computer Emergency Response*

Team (CERT), *Common Weakness Enumeration* (CWE), *SysAdmin, Audit, Network, Security* (SANS) i OWASP te kontinuirano provodi sigurnosnu obuku svojih zaposlenika [20].

U fazi testiranja proizvoda Huawei je projektirao testne slučajeve na temelju modeliranja prijetnji kako bi provjerio učinkovitost osmišljenih mjera za ublažavanje prijetnji. Huawei je usvojio sigurnosni mehanizam provjere tzv. "mnogo očiju i mnogo ruku". Pored sigurnosnih testova proizvoda Huawei je osnovao neovisni kibernetički sigurnosni laboratorij, neovisan o odjelu istraživanja i razvoja, odgovoran za konačnu provjeru proizvoda. Rezultati testova se direktno prijavljuju osobi odgovornoj za kibernetičku sigurnost i privatnost koja ima pravo zabraniti lansiranje proizvoda. Sheme testiranja i provjere trećih strana podržane su uz suradnju kupaca i regulatornih tijela [20].

Osim toga, poduzimaju se mjere za povećanje sigurnosti softvera, na primjer, sigurnosne opcije softverskog prevoditelja (engl. *compiler*) se koriste u procesu izrade, a sigurnosno skeniranje se provodi prije objavljivanja verzije. Centar za digitalni potpis potpisuje svaki softver te se može koristiti za provjeru cjelovitosti prije njegova učitavanja. Ovaj mehanizam sprječava neovlašteno mijenjanje ili zamjenu softvera [20].

Huawei se ne zalaže samo za izgradnju povjerljivosti, cjelovitosti, dostupnosti, praćenja i zaštite privatnosti korisnika u 5G opremi na temelju 3GPP standarda, već i za suradnju s operatorima radi stvaranja visoke kibernetičke otpornosti u mrežama. Za zaštitu 5G mrežne opreme Huawei pruža sljedeće ublažavajuće sigurnosne mjere temeljene na standardima:

- u mreži operatora, zone unutar podatkovnog centra s različitim razinama sigurnosti projektirane su na temelju usluga. Svaka je zona izolirana vatrozidom. Korisnici ne mogu izravno pristupiti zonama s višom razinom sigurnosti [20].
- U sigurnosnoj zoni, domene se obično koriste za daljnju klasifikaciju i izolaciju usluga. Na primjer, mrežne usluge operatora općenito se dijele na operativnu i upravljačku domenu, domenu povezivanja, kontrolnu domenu i podatkovnu domenu. Različite vrste usluga združene su u različite domene. Domene su međusobno izolirane vatrozidima i dopušten je samo ovlašteni pristup [20].
- U okruženju s više dobavljača potrebna je izolacija računala unutar domene. Na istom računalu se za daljnju izolaciju mogu koristiti sigurnosne izolacijske sheme virtualnih strojeva, virtualizacijskog sloja, procesora, memorije i mreže [20].

Oprema podržava praćenje i reviziju sigurnosti sustava. Oprema podržava sigurno pokretanje kako bi se spriječilo neovlašteno mijenjanje tijekom pokretanja sustava te provjeru cjelovitosti važnih softverskih datoteka i pokrenutog kôda kako bi se spriječilo neovlašteno mijenjanje tijekom izvođenja. Time se poboljšava zaštita cjelovitosti sustava [20].

Huawei nudi sigurnosno rješenje HiSec za podršku kibernetičke otpornosti s kraja na kraj koje obuhvaća upravljanje sigurnošću, otkrivanje i analizu prijetnji te odgovor i oporavak. Rješenje se temelji na smjernici NIST CSF kroz šest ključnih tehnologija: učinkovito upravljanje ranjivostima, zaštita sustava na temelju čipova, prilagodljiva sigurnost podataka, inteligentno otkrivanje prijetnji, automatiziran odgovor na prijetnju i omogućavanje otvorenog sigurnosnog sustava [20].

Što se tiče zaštite privatnosti, 5G sustavi zahtijevaju mjere za zaštitu privatnosti s kraja na kraj na temelju zahtjeva GDPR-a:

- 3GPP 5G standard definira kriptiranje korisničkih identiteta tijekom prijenosa radio sučeljem, a kriptiranje i zaštita cjelovitosti se provode s kraja na kraj prijenosnog kanala kako bi se spriječila krađa ili izmjena osobnih podataka.
- Zaštita podataka korisničke ravnine: i zračno sučelje i prijenosni kanal podržavaju kriptiranje i zaštitu cjelovitosti prema 3GPP standardima.
- Kod prikupljanja podataka o identitetu korisnika potrebne su sljedeće mjere:
  - Sve se korisničke radnje moraju odobriti prije prikupljanja podataka.
  - Prikupljeni podaci se kriptiraju tijekom pohrane i obrade radi sprječavanja krađe podataka. Podaci se automatski brišu po isteku roka za pohranu osobnih podataka.
  - U slučaju popravka opreme, osiguran je mehanizam sigurnog brisanja podataka prije povratka proizvođaču radi sprječavanja krađe podataka tijekom popravka.
- Mora se dostaviti dokumentacija koja opisuje način na koji mrežna oprema upravlja osobnim podacima u odnosu na zahtjeve privatnosti [20].

Huawei ima kibernetičke sigurnosne transparentne centre u Europi i Kini. 5. ožujka 2019. Huawei je otvorio kibernetički sigurnosni transparentni centar u Bruxellesu s tri osnovne funkcije [52]. Prva se odnosi na pružanje uvida u kibernetičke sigurnosne prakse s kraja na kraj, od strategije i opskrbnog lanca do istraživanja i razvoja te proizvoda i rješenja u području 5G mreže, IoT uređaja i oblaka. Drugo, centar će olakšati komunikaciju između Huaweija i ključnih sudionika na temu strategija kibernetičke sigurnosti i sigurnosti s kraja na kraj te praksi zaštite privatnosti. Huawei će surađivati s industrijskim partnerima na istraživanju i promicanju razvoja sigurnosnih standarda i mehanizama provjere kako bi se olakšale tehnološke inovacije u kibernetičkoj sigurnosti u cijeloj industriji. Treće, centar će korisnicima Huaweija pružiti platformu za testiranje i provjeru sigurnosti proizvoda te srodne usluge [52].

Osim u Europi, Huawei je 9. lipnja 2021. otvorio najveći transparentni centar za kibernetičku sigurnost i zaštitu privatnosti u kineskom Dongguanu gdje su sa cijelom industrijom podijelili svoj osnovni sigurnosni okvir [53].

5. Povijesni incidenti

Ranjivosti mrežne opreme tvrtki Ericsson i Huawei uzrokovale su maliciozne radnje poput prisluškivanja i krađe podataka. U nastavku su opisani neki od otkrivenih incidenata.

5.1 Afera u Grčkoj

U razdoblju od kolovoza 2004. do 24. siječnja 2005. [54] u Grčkoj su prisluškivani, a vjerojatno i snimani telefonski razgovori premijera, ministra obrane i vanjskih poslova, grčkog povjerenika za EU, gradonačelnika Atene, zaposlenika američke ambasade, najviših vojnih i policijskih službenika i mnogih drugih [55]. 9. ožujka 2005. je pronađeno tijelo Costasa Tsalikidisa koji je bio zadužen za mrežno planiranje u tvrtki Vodafone čiji su pretplatnici bili žrtve napada. Veza njegove smrti, za koju se sumnja da je samoubojstvo, s ovim napadom nije utvrđena.

Početkom 2003. tehničari Vodafonea su s inženjerima Ericssona ažurirali preklopnike što je uključilo i softver za udaljeno upravljanje kojim se mogu pratiti glasovni i podatkovni tokovi njihovim dupliciranjem i preusmjeravanjem, ali uz uvjet da ih je pokrenuo Ericssonov sustav presretanja (engl. *Interception Management System*, IMS). IMS se pokreće isključivo uz sudski nalog. Izazov napadača je bio neprimjetno zaobići korištenje IMS-a što su postigli instaliranjem niza zakrpa na 29 zasebnih blokova kôda. Prisluškivani brojevi su bili pohranjeni u izoliranu memoriju samog softvera unutar memorije preklopnika. Kôd je izmijenjen na način da se u popisu aktivnih procesa nije prikazivao. Softverom su napravljena i stražnja vrata putem kojih su napadači imali pristup. Sve radnje napadača su ostale skrivene upisivanjem bezazlenih naredbi praćenih sa šest razmaka kojim se deaktiviralo zapisivanje transakcijskih dnevnika, spriječilo pokretanje alarma zbog deaktivacije te omogućilo izvršavanje naredbi za presretanje poziva [54]. Softver je instaliran na četiri Ericssonova preklopnika. Stvarao je paralelne glasovne tokove, jedan između izvornih sudionika razgovora, a drugi, kopiju prvog kojeg je slao na mobilni uređaj gdje je prisluškivan i vjerojatno sniman. Lokaciju prisluškivanog broja je softver automatski slao SMS porukom.

24. siječnja 2005. napadači su ažurirali softver čime su automatske poruke o lokaciji prisluškivanih brojeva ostale neisporučene što se zabilježilo na preklopniku i pokrenulo istragu. Inženjeri tvrtke Ericsson su u redovitim *dump*-ovima (sirovi podaci iz memorije računala) pronašli popis prisluškivanih brojeva, vremena presretanja, izolirali umetnuti softver i analizirali ga u testnom okruženju.

7. ožujka 2005. je Vodafone deaktivirao zlonamjerni softver što je gotovo sigurno upozorilo napadače dajući im priliku da isključe uređaje na koje su preusmjeravali pozive. Istražitelji nisu uspjeli pronaći lokaciju mobilnih uređaja napadača i uhvatiti ih na djelu.

Dok je analiza bila u tijeku, u lipnju 2005. inženjeri tvrtke Vodafone su ažurirali dva od tri poslužitelja za pristup sustavu upravljanja razmjene (engl. *exchange management system*) čime su pobrisani svi zapisi pristupanja sustavu i suprotno politikama, nisu sačuvane pričuvne kopije.

Zapisi o softveru su mogli biti trajnije pohranjeni, ali zbog manjka prostora na disku i prioriteta čuvanja podataka o naplati, čuvani su samo pet dana. Nadalje, nisu izravno pozvani organi za provođenje zakona niti neovisno tijelo za sigurnost i privatnost, već je Vodafone kontaktirao direktno premijerov ured. Nikada nisu otkriveni počinitelji niti je li napad bio organiziran iznutra ili izvana.

Kod ovakvih napada u kojima je narušena privatnost i povjerljivost podataka, malo se toga može napraviti da se nastala šteta ublaži. Nužno je djelovati proaktivno, razvijati sigurnosna rješenja, redovito ih testirati na sigurnosne ranjivosti te kriptirati podatke cijelim putem [54].

5.2 Krađa intelektualnog vlasništva tvrtke Nortel

Kanadska tvrtka Nortel je osnovana 1895. Bila je proizvođač telekomunikacijske i podatkovne mrežne opreme. Kontrolirala je tisuće patenata za optička vlakna i bežičnu mrežu te izumila bežični uređaj s ekranom osjetljivim na dodir gotovo desetljeće prije iPhonea. Kasnih 1990-ih kanadska sigurnosno-obavještajna služba je uočila "neobičan promet", krađu podataka i dokumenata iz Ottawe. Upozorili su čelnike Nortela o krađi njihovog intelektualnog vlasništva, no oni nisu ništa učinili. 2004. su hakeri u Kini ukrali lozinku izvršnog direktora Nortela, Franka Dunna i 6 zaposlenika iz odjela za optiku. Koristeći skriptu nazvanu *Il. browse*, ukrali su podatke Nortelovih odjela za razvoj proizvoda, istraživanje i razvoj, projektne dokumente, zapisnike itd. Na IP adresu registriranu na tvrtku *Shanghai Faxian Corp.* je poslano oko 800 dokumenata. Nortel nikada nije pokušao utvrditi kako su lozinke ukradene, već su ih samo izmijenili. Hakerski napadi su se nastavili i do početka 2009. tvrtka je bila u stečaju.

Dok je Nortel propadao, Huawei je angažirao oko 20 Nortelovih znanstvenika koji su razvijali temelje za 5G tehnologiju. Tako je Wen Tong, danas glavni tehnološki direktor za bežičnu tehnologiju u Huaweiju, do 2009. bio voditelj Laboratorija za mrežnu tehnologiju u Nortelu. Tong je 2009. predvodio egzodus inženjera i znanstvenika iz Nortela u Huawei [56].

5.3 Ranjivost mrežne opreme u Italiji

Važnost testiranja opreme na sigurnosne ranjivosti potvrđena je na primjeru usmjernika kineske tvrtke Huawei koje su talijanski pretplatnici operatora Vodafone koristili kao kućne internetske usmjernike u razdoblju od 2009. do 2011. Vodafone je zbog konkurentnih cijena počeo kupovati WiFi usmjernike od Huaweija 2008. za talijansko tržište, a kasnije i za Ujedinjeno Kraljevstvo, Njemačku, Španjolsku i Portugal.

U siječnju 2011. je za Vodafone u Italiji neovisni izvođač proveo sigurnosno testiranje opreme i otkrio na usmjernicima aktivan i dostupan servis *telnet* kojim se podaci prenose nekriptirano, u čitkom obliku, čime je moguć pristup upravljanju usmjernika i uređajima spojenim na taj usmjernik. Vodafone nije tražio *telnet* u svojim zahtjevima za usmjernike i od Huaweija je zatražio

uklanjanje otkrivenog propusta. Iako su iz Huaweija tvrdili da je *telnet* uklonjen, Vodafone je testiranje ponovio i ponovno ga detektirao. Huawei je potom odbio ukloniti servis pozivajući se na proizvodne zahtjeve i potrebe *telneta* za konfiguriranje podataka o uređaju i provođenje testova, uključujući WiFi te ponudio ukidanje servisa nakon provedenih koraka. Nisu pronađeni zapisi o pristupanju putem tog servisa [57].

5.4 Zlonamjerni kôd u opremi australskog operatora

2012. godine australska obavještajna služba je otkrila sofisticirani upad u telekomunikacijske sustave zemlje koji je započeo ažuriranjem softvera opreme tvrtke Huawei velikog australskog operatora *Singtel Optus Pty Limited*. Ažuriranje je uključilo zlonamjerni kôd koji je reprogramirao zaraženu opremu na način da bilježi svu komunikaciju koja prolazi kroz nju i šalje ju u Kinu. Podaci su omogućili pristup sadržaju privatne komunikacije i informacijama koje bi se mogle koristiti za ciljanje određenih ljudi ili uređaja u budućim napadima. Nakon nekoliko dana kôd se izbrisao zbog čega su forenzika i pronalaženje dokaza bili otežani.

Australske obavještajne agencije utvrdile su da su za krađu podataka odgovorne kineske špijunske službe koje su se infiltrirale u redove Huaweijevih tehničara koji su pomogli u održavanju opreme i pokrenuli ažuriranje softvera [58].

Australija je 2018. zabranila opremu tvrtke Huawei u svojoj 5G mreži. Ključni razlog zabrane je bila analiza ranjivosti njihovih proizvoda po kojoj je procijenjeno više od 300 zasebnih rizika koje treba ublažiti kako bi se oprema mogla sigurno koristiti [58].

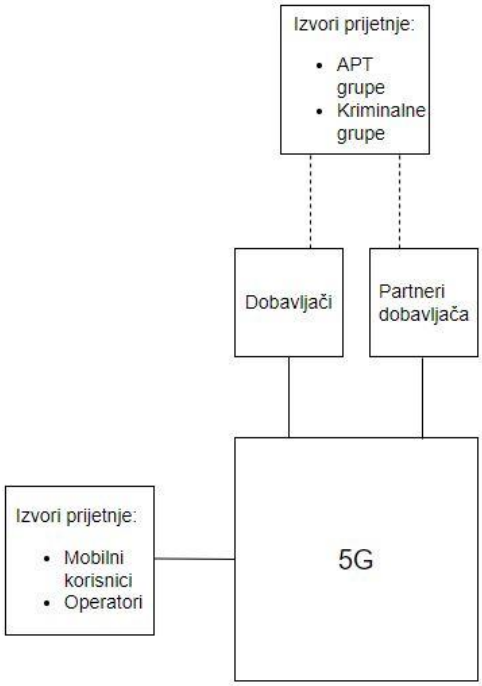
6. Oprema i usluge tvrtki iz Kine – prijetnje, rizici i mjere za ublažavanje rizika

Huawei je najveći svjetski dobavljač telekomunikacijske opreme [59] i ima svoju opremu implementiranu diljem svijeta, dominantno u Kini, Južnoj Africi i Južnoj Americi. Oprema je povoljnija od konkurentske, a nude i subvencionirane zajmove za financiranje izgradnje kineske infrastrukture, posebno u zemljama u razvoju [60]. Osim dominacije globalnim tržišnim udjelom u 5G infrastrukturi, kineski prioritet je razviti što više patenata koje bi 3GPP usvojio u standard za 5G. Time će osigurati ovisnost tržišta o njihovoj opremi i uslugama. Tako je 2016. Huawei predložio, a 3GPP u standard za 5G usvojio polarno kodiranje, ispravljanje pogreški na vezi tijekom prijenosa podataka.

U ovom poglavlju analizirat će se izvori prijetnje, ranjivosti i prijetnje kineske opreme, potencijalni rizici te mjere za njihovo ublažavanje.

6.1 Izvori prijetnji

Sigurnost 5G mreže može ugroziti nenamjerna i/ili zlonamjerna radnja. Vektori napada na 5G su brojni, a na Slika 6.1 su prikazani mogući izvori prijetnje. 5G mobilni korisnici i operatori predstavljaju prijetnju na 5G sigurnost, ali njihov utjecaj nije značajan i nije razmatran u ovom radu. Pretpostavka je kako mobilni korisnici nemaju dovoljna znanja niti alate da bi značajno ugrozili sigurnost 5G mreže. Cilj operatora je pružiti stabilnu i sigurnu 5G mrežu i prijetnje s njihove strane su većinom nenamjerne. Osim dobavljača opreme i njihovih partnera, ozbiljnu prijetnju predstavljaju kriminalne grupe i dobro organizirane grupe ljudi koje se nazivaju naprednim ustrajnim prijetnjama (engl. *Advanced Persistent Threat,* APT). APT grupe posjeduju napredna znanja i alate za izvođenje sofisticiranih računalnih napada koji traju dulje vremensko razdoblje, a usmjereni su protiv vlada, kompanija i političkih aktivista [61]. U 5G-u APT-ovi mogu provesti napade preko dobavljača opreme ili partnera dobavljača u ciljanoj zemlji. APT-ove može angažirati i vlast zemlje što je posebno značajno za Kinu i kinesku legislativu koja će biti opisana u nastavku radu.



Slika 6.1 Izvori prijetnje na 5G

6.2 Ranjivosti i prijetnje

Ranjivosti opreme se najviše odnose na stražnja vrata, prikupljanje podataka, krađu intelektualnog vlasništva i sl. U nastavku su opisane prijetnje koje mogu uzrokovati kineski zakoni, ranjivosti kineske opreme i/ili usluga.

6.2.1 Zakon o zaštiti osobnih podataka Narodne Republike Kine

Zakon o zaštiti osobnih podataka Narodne Republike Kine je prihvaćen 20. kolovoza 2021., a na snagu je stupio 1. studenog 2021. Zakonom se nastoje zaštititi osobni podaci, standardizirati aktivnosti rukovanja osobnim podacima i promicati racionalnu uporabu osobnih podataka. Zakon se primjenjuje na upravljanje osobnim podacima fizičkih osoba unutar granica Narodne Republike Kine, a izvan granica je primjenjiv u ovim slučajevima:

- pružanje proizvoda ili usluga fizičkim osobama unutar granica,
- analiza ili procjena aktivnosti fizičkih osoba unutar granica,
- druge okolnosti predviđene zakonima ili administrativnim propisima [62].

U nastavku su izdvojeni članci zakona koji se tiču kineskih dobavljača 5G opreme i njihove obvezne usklađenosti sa zakonom.

U članku 4 je definiran osobni podatak: osobni podaci su sve vrste informacija, zabilježene elektroničkim ili drugim sredstvima, vezane za identificirane ili prepoznatljive fizičke osobe, ne uključujući anonimizirane podatke. Rukovanje osobnim podacima uključuje prikupljanje, pohranu, uporabu, obradu, prijenos, pružanje, otkrivanje, brisanje osobnih podataka itd. [62].

Člankom 5 se zabranjuje rukovanje osobnim podacima na obmanjujući, lažni, prisilni ili druge načine [62].

Članci 7 i 10 definiraju rukovanje osobnim podacima: kod rukovanja osobnim podacima poštuju se načela otvorenosti i transparentnosti, otkrivaju se pravila rukovanja osobnim podacima te se jasno ukazuje svrha, način i opseg rukovanja. Nijedna organizacija ili pojedinac ne smije nezakonito prikupljati, koristiti, obrađivati, prenositi, prodavati, kupovati, pružati ili otkrivati osobne podatke drugih osoba niti se smije baviti aktivnostima rukovanja osobnim podacima koje štete nacionalnoj sigurnosti ili javnom interesu [62].

Članak 12 uključuje i međunarodnu suradnju: država snažno sudjeluje u formuliranju međunarodnih pravila ili normi o zaštiti osobnih podataka, potiče međunarodnu razmjenu i suradnju na području zaštite osobnih podataka te promiče međusobno priznavanje pravila ili normi o zaštiti osobnih podataka, standarda itd. s drugim zemljama, regijama i međunarodnim organizacijama [62].

U članku 28 se praćenje lokacija fizičkih osoba smatra osjetljivim osobnim podatkom: osjetljivi osobni podaci označavaju osobne podatke koji, nakon što su procurili ili se nezakonito upotrijebili, mogu lako uzrokovati povredu dostojanstva fizičkih osoba teškom štetom po osobnu ili imovinsku sigurnost, što uključuje podatke o biometrijskim karakteristikama, vjerskim uvjerenjima, posebno određenom statusu, medicinskom zdravlju, financijskim računima, praćenje lokacije pojedinca kao i osobne podatke maloljetnih osoba mlađih od 14 godina [62].

Članak 36 definira pohranu osobnih podataka: osobni podaci kojima rukuju državni organi pohranit će se na kopnenom teritoriju Narodne Republike Kine. Ako je osobne podatke potrebno dostaviti u inozemstvo, provest će se sigurnosna procjena za koju se može zatražiti podrška i pomoć od nadležnih tijela [62].

Temeljem članka 42 Kina može ograničiti ili zabraniti ustupanje osobnih podataka stranim organizacijama ili pojedincima: „tamo gdje strane organizacije ili pojedinci sudjeluju u rukovanju osobnim podacima kršeći prava i interese građana Narodne Republike Kine ili nanoseći štetu nacionalnoj sigurnosti ili javnom interesu Narodne Republike Kine, Državni odjel za kibernetičku sigurnost i informatizaciju im može izdati upozorenje, ograničiti ili zabraniti pružanje osobnih podataka itd. [62]“.

Člankom 63 se oprema kojom se nezakonito rukuje osobnim podacima može zapečatiti ili oduzeti: relevantni odjeli Državnog vijeća koji ispunjavaju dužnosti i odgovornosti u pogledu zaštite osobnih podataka mogu, među ostalim, donijeti sljedeće mjere:

- provođenje ispitivanja na licu mjesta i provođenje istraga nad osumnjičenim nezakonitim aktivnostima rukovanja osobnim podacima,

- ispitivanje opreme i predmeta relevantnih za aktivnosti rukovanja osobnim podacima; kad postoje dokazi uporabe opreme ili predmeta u svrhu nezakonitih aktivnosti rukovanja osobnim podacima, nakon što pismeno prijave glavnoj osobi svog odjela i dobiju odobrenje, mogu ih zapečatiti ili oduzeti [62].

U članku 66 su definirane kazne zbog neusklađenosti s odredbama ovog zakona: „tamo gdje se s osobnim podacima rukuje suprotno ovom zakonu ili se s njima rukuje bez ispunjavanja obveze zaštite osobnih podataka u skladu s odredbama ovog zakona, prethodno spomenuti odjeli moraju narediti provedbu usklađivanja sa zakonom, oduzeti nezakoniti prihod i naložiti privremenu obustavu ili prestanak pružanja usluga aplikacijskih programa koji nezakonito rukuju osobnim podacima; ako se provedba usklađivanja odbije, dodatno će se izreći novčana kazna u iznosu od najviše 1 milijun kineskih juana; izravno odgovorna osoba i drugo izravno odgovorno osoblje kaznit će se novčanom kaznom u iznosu od 10.000 do 100.000 kineskih juana. Ako su okolnosti nezakonitih radnji spomenutih u prethodnom stavku ozbiljne, treba narediti provedbu usklađivanja sa zakonom, oduzeti nezakoniti prihod i izreći novčanu kaznu u iznosu od najviše 50 milijuna kineskih juana ili 5% godišnjeg prihoda. Također se može naložiti obustava povezanih poslovnih aktivnosti ili prestanak poslovanja radi usklađivanja sa zakonom te izvršiti prijava nadležnom odjelu radi poništenja odgovarajućih administrativnih ili poslovnih dozvola [62].“

Zaključno, važno je naglasiti odredbu iz članka 2 zakona: „niti jedna organizacija ili pojedinac ne smije povrijediti prava i interese fizičkih osoba [62]“.

6.2.2 Zakon o kibernetičkoj sigurnosti Narodne Republike Kine

Zakon o kibernetičkoj sigurnosti Narodne Republike Kine je na snazi od 1. lipnja 2017. Zakon zahtijeva od mrežnih operatora potpuni pristup podacima i tehničku podršku na zahtjev vlasti. Zakon također nameće obvezna testiranja i certifikaciju računalne opreme za mrežne operatore kritičnih sektora - komunikacije, informacijske usluge, energija, prijevoz, voda, financijske usluge, javne usluge i elektroničke državne usluge [63].

Dužnost prihvaćanja nadzora kineske vlade nad mrežnim operatorima naveden je u članku 9 zakona: mrežni operatori dužni su pri obavljanju poslovnih djelatnosti i pružanju usluga pridržavati se zakona i administrativnih propisa, poštivati društveni moral, poštivati poslovnu etiku, poslovati u dobroj vjeri, izvršavati svoje obveze u zaštiti kibernetičke sigurnosti, prihvatiti nadzor vlade i javnosti te preuzeti društvenu odgovornost [64].

Člankom 22 je dobavljačima opreme zabranjeno instalirati zlonamjerni softver: mrežni proizvodi i usluge moraju biti u skladu s obveznim zahtjevima relevantnih nacionalnih standarda. Pružatelji mrežnih proizvoda i usluga ne smiju instalirati zlonamjerni softver. Kada davatelj usluga otkrije sigurnosni propust ili ranjivost u svojim mrežnim proizvodima ili uslugama, odmah će poduzeti mjere sanacije i slijediti odredbe poput informiranja korisnika i prijave incidenta nadležnima. Pružatelji mrežnih proizvoda i usluga pružat će usluge održavanja sigurnosti u predviđenom razdoblju ili razdoblju dogovorenom između relevantnih strana. Ako mrežni proizvod ili usluga

prikuplja podatke korisnika, pružatelj će to jasno naznačiti i dobiti suglasnost korisnika. Ako se radi o osobnim podacima korisnika, pružatelj će se također pridržavati odredbi ovog zakona, odredbi relevantnih zakona i administrativnih propisa o zaštiti osobnih podataka [64].

Članak 23 definira certifikaciju kritične mrežne opreme: kritična mrežna oprema i specijalizirani kibernetički sigurnosni proizvodi trebaju, u skladu s obveznim zahtjevima relevantnih nacionalnih standarda, biti certificirani od strane kvalificirane institucije ili ispunjavati zahtjeve sigurnosne inspekcije prije prodaje ili pružanja usluge [64].

Sigurnosne obveze mrežnih operatora na nacionalnoj razini definirane su u članku 28: mrežni operatori će pružiti tehničku podršku i pomoć tijelima javne sigurnosti i nacionalne sigurnosti radi očuvanja nacionalne sigurnosti i istrage kriminalnih aktivnosti [64].

Člankom 37 je definirano gdje operatori kritične informacijske infrastrukture trebaju pohraniti i eventualno dostaviti osobne podatke: operatori kritične informacijske infrastrukture koji prikupljaju ili kreiraju osobne ili važne podatke tijekom rada na kopnenom teritoriju Narodne Republike Kine pohranit će takve podatke unutar granica kopnene Kine. Ako je takve podatke potrebno dostaviti van tog teritorija, provest će se sigurnosna procjena prema mjerama koje su zajednički formulirala nacionalna tijela za kibernetički prostor i relevantni odjeli Državnog vijeća. Tamo gdje zakoni ili administrativni propisi propisuju drugačije, primijenit će se te odredbe [64].

Člankom 44 se zabranjuje krađa osobnih podataka: pojedinci ili organizacije ne smiju krasti niti koristiti druga nezakonita sredstva za dohvat osobnih podataka te ne smiju nezakonito prodavati ili nezakonito davati osobne podatke drugima [64].

6.2.3 Zakon o tvrtkama Narodne Republike Kine

Zakon o tvrtkama Narodne Republike Kine je usvojio Nacionalni narodni kongres Narodne Republike Kine 29. prosinca 1993., a stupio je na snagu 1. srpnja 1994. Od tada je nekoliko puta mijenjan. Najnovija verzija zakona stupila je na snagu 2018. Zakon uređuje društva s ograničenom odgovornošću i dionička društva [65].

Za potrebe ovog rada izdvojena su četiri članka od kojih su zadnja dva značajna i daju uvid u utjecaj i prisutnost kineske vlade u tvrtkama:

- Članak 1: zakon je donesen radi standardizacije organizacije i aktivnosti tvrtki, zaštite zakonitih prava i interesa tvrtki, dioničara i vjerovnika, zaštite društvenog i ekonomskog poretka te promicanja razvoja socijalističkog tržišnog gospodarstva [66].
- Članak 2: tvrtka se odnosi na društva s ograničenom odgovornošću i dionička društva koja su osnovana na teritoriju Kine u skladu sa zakonom [66].
- Članak 5: tvrtka mora prihvatiti nadzor vlade, prilikom obavljanja poslovnih aktivnosti, tvrtka se mora pridržavati zakona i administrativnih propisa, poštivati društveni moral i poslovnu etiku, ponašati se u dobroj vjeri, prihvatiti nadzor vlade i javnosti i snositi društvenu odgovornost [66].

- Članak 19: tvrtka će osnovati organizaciju Komunističke partije Kine koja će obavljati djelatnosti stranke u skladu sa statutom Komunističke partije Kine. Tvrtka će osigurati potrebne uvjete za aktivnosti stranačke organizacije [66].

6.2.4 Nacionalni obavještajni zakon Narodne Republike Kine

Nacionalni obavještajni zakon Narodne Republike Kine upravlja kineskim obavještajnim i sigurnosnim aparatom, a na snagu je stupio 27. lipnja 2017. Najkontroverzniji članak zakona je 7., koji potencijalno prisiljava tvrtke koje posluju ili su registrirane u Kini na predaju informacija kineskim obavještajnim agencijama: sve organizacije i građani podržavat će, pomagati i surađivati s nacionalnim obavještajnim naporima u skladu sa zakonom te štititi tajne nacionalnog obavještajnog rada kojih su svjesni [67].

Isti je zakon člankom 10 primjenjiv i izvan kineskog teritorija što implicira na kineske tvrtke koje posluju u inozemstvu, posebno tehnološke, prisiljavajući ih na predaju korisničkih podataka čak i kada posluju u stranim jurisdikcijama: prema potrebi, nacionalne obavještajne institucije moraju koristiti potrebna sredstva, taktike i kanale za provođenje obavještajnih napora, u zemlji i inozemstvu [67].

6.2.5 Zakon o protušpijunaži Narodne Republike Kine

Zakon o protušpijunaži Narodne Republike Kine stupio je na snagu 1. studenog 2014. Zakon je formuliran na temelju Ustava s ciljem sprječavanja, zaustavljanja i kažnjavanja špijunskog ponašanja i očuvanja nacionalne sigurnosti [68].

Člankom 22 zakona se od tvrtki i pojedinaca traži bezuvjetno ustupanje podataka u slučaju prikupljanja dokaza ili istrage o špijunaži: kada organi državne sigurnosti provode istragu o špijunskom ponašanju ili prikupljaju bitne dokaze, relevantne tvrtke i pojedinci će iste bez odbijanja iskreno ustupiti [68].

6.2.6 Kršenje ljudskih prava - aplikacija Xuexi Qiangguo

U Kini je od 2019. u širokoj primjeni edukacijska aplikacija Xuexi Qiangguo (engl. *Study the great Nation*) koju koristi preko 100 milijuna korisnika. Aplikaciju je razvio Partijski odjel za propagandu uz pomoć kineske tvrtke Alibaba. Cilj aplikacije je usaditi stavove kineskog čelnika, indoktrinirajući naciju „mislima Xi Jinpinga“ i prisiliti na lojalnost kineskoj Komunističkoj partiji. Vlada potiče Kineze na aktivnu uporabu aplikacije, rješavanje ispita, čitanje članaka čime se "zarađuju" bodovi. Aplikacija je obvezna za stranačke dužnosnike i državne službenike dok na nekim radnim mjestima korištenje aplikacije određuje iznos plaće. Prilikom instalacije korisnici

moraju dati privolu za pristup osobnim podacima, kameri, mikrofonu, zapisima poziva i lokaciji [60].

Njemačka tvrtka Cure53 je u kolovozu 2019. provela procjenu aplikacije na Android operativnom sustavu s Europskom konvencijom o ljudskim pravima [69] kao osnovom. Pronađeno je šest ranjivosti od kojih jedna dokazano krši ljudska prava, tri predstavljaju evidentno kršenje ljudskih prava dok su dvije ranjivosti okarakterizirane nejasnima u pogledu implikacija na ljudska prava [70].

Aplikacija prikuplja sljedeće podatke:

• informacije o mobilnom uređaju (jedinstveni broj mobilnog uređaj (engl. *International Mobile Equipment Identity*, IMEI), model, ID uređaja, omogućen puni pristup operativnom sustavu),

• informacije o konekcijama (identifikator WiFi mreže, operator, virtualna privatna mreža (engl. *Virtual Private Network*, VPN),

• informacije o korisniku (UID, kolačići, ID sesija, pozivi, statistike poziva, kontakti),

• lokaciju,

• pokrenute procesi i servise.

Aplikacija provjerava koje su od 960 specifičnih aplikacija instalirane na mobilnom uređaju. Primjeri aplikacija koje se skeniraju su Tripadvisor, Airbnb, WhatsApp, Kakao Talk, Facebook Messenger, Skype, Baidu mape, Uber, Amazon Kindle, aplikacije mobilnog bankarstva, Disney igra „Temple Run“.

Jedna od evidentnih ranjivosti se odnosi na korištenje slabih kriptografskih algoritama u dijelu koji sadrži informacije o biometrijskim podacima i e-pošti korisnika što omogućuje njihovo učinkovito prikupljanje i analizu u centraliziranoj bazi podataka.

Otkriveno je da se zapisi šalju svakodnevno na domenu xuexi.cn koja je u vlasništvu tvrtke Alibaba i jednim dijelom na domenu qq.com čijim serverima upravlja kineska tvrtka Tencent, prodavač videoigara [70].

6.2.7 Otkrivene ranjivosti opreme tvrtke Huawei

Američka tvrtka Finite State koja se bavi sigurnosnom analizom firmvera provela je 2019. procjenu rizika više od 500 mrežnih uređaja tvrtke Huawei [71]. Analiza je tražila ranjivosti poput kodiranih vjerodajnica za stražnja vrata, nesigurnu upotrebu kriptografskih ključeva, pokazatelje nesigurnih praksi razvoja softvera, poznate ranjivosti i nepoznate (*0-day*) ranjivosti. Ranjivosti, bile one namjerne ili nenamjerne, otkrivene su na svakom analiziranom uređaju.

1. Huawei svoje komponente ne ažurira redovito. Prosječna starost komponenti firmvera treće strane je 5,36 godina. Pronađeno je tisuće primjera komponenti starijih od 10 godina poput verzije biblioteke OpenSSL [71].

2. Poznate ranjivosti (engl. *Common Vulnerabilities and Exposures*, CVE [72]) su otkrivene u najnovijim verzijama firmvera. Prosječan broj CVE-ova po firmveru je 102. 27% otkrivenih CVE-ova ima ocjenu između 7.0 i 8.0 (visoka ranjivost) ili 9.0 i 10.0 (kritična ranjivost). Ove ranjivosti mogu dovesti do potpunog ugrožavanja zahvaćenih sustava [71].

3. U 29% svih analiziranih firmvera je otkrivena barem jedna zadana vjerodajnica. Huawei koristi autentifikaciju temeljenu na Linux operativnom sustavu. Korisnička imena ukazuju na to da su mnogi od njih testni računi koje je Huawei ili dobavljač softvera treće strane ostavio u firmveru. Primjeri računa sa zadanom vjerodajnicom su user, ftpvrpv8, admin, enspire, factory, factory0, factory1, fae, sshusr, default, huawei, Admin, root0, root1. Zlonamjerni akter bi to mogao iskoristiti i ostvariti privilegirani pristup uređaju na mreži [71].

4. U 8 firmvera je otkrivena datoteka *authorized_keys* koja može omogućiti pristup uređaju kroz stražnja vrata. *Authorized_keys* je datoteka u Linuxu u kojoj su zapisani ključevi za *Secure Shell* (SSH) koji se koriste za udaljeno spajanje na uređaj. Ključevima u ovoj datoteci je omogućen trajni pristup uređaju svakome tko posjeduje privatni ključ. SSH ključevi se koriste kao sredstvo identifikacije korisnika na udaljenom računalu korištenjem kriptografije javnog ključa. U ovoj metodi javni ključevi su široko rasprostranjeni, a privatni ključ posjeduje samo vlasnik tj. osoba koja se udaljeno spaja na uređaj. Za iskorištavanje ove ranjivosti potreban je aktivan servis SSH koji operatori iz sigurnosnih razloga mogu onemogućiti [71].

5. U samo 34,97% firmvera je uključena zaštita pokretanja izvršnog kôda na način da se kôd učita na nepredviđeno mjesto. Time se zlonamjerni pokušaji mogu lakše detektirati i upozoriti operatora. 73.96% firmvera je imalo uključeno rješenje za sprječavanje izvršenja podataka kojim se dijelovi memorije označavaju kao neizvršne [71].

6. Sigurne funkcije se koriste u manje od 17% pozivanja funkcija. Postoje nesigurne funkcije koje se klasificiraju kao memorijske operacije, operacije s nizovima, funkcije ispisa, izvršavanje programa i operacije s datotekama. Većina od 20 najčešće korištenih nesigurnih funkcija u firmverima je povezana s memorijom i nizovima. Korištenje ovih funkcija, osobito kada su sigurnije alternative dostupne već duže od desetljeća, može ukazivati na zanemarivanje sigurnih razvojnih praksi [71].

7. Novija verzija firmvera preklopnika je ranjivija od prethodne. Verzije su izdane u razmaku od dvije godine. Povećan je broj CVE-ova i zlouporabe memorije čime su ažurirani uređaji postali nesigurniji [71].

6.3 Rizici

Kinezi bi pomoću svoje opreme i povezanih proizvoda diljem svijeta mogli pristupiti privatnim podacima milijardi ljudi, prikupljati privatne podatke o povijesti bolesti pojedinaca, potrošačkim navikama, političkim stavovima, iskazanim osobnim podacima na društvenim mrežama, fizičkoj lokaciji, financijskoj situaciji itd. Pristup takvim informacijama mogao bi se

koristiti na razne načine, uključujući stjecanje komercijalne ili tehničke prednosti na tržištima temeljenim na podacima ili kompromitiranje osoba u politici [60].

Ranjivosti u kineskoj opremi, ukoliko se ne prepoznaju i ne ublaže, mogu dovesti do prekida rada dijela 5G opreme ili dijela 5G mreže što predstavlja rizik na nacionalnoj razini i može dovesti do kibernetičke krize (ugroza sigurnosti ljudi, demokratskog sustava, političke stabilnosti, gospodarstva, okoliša i drugih nacionalnih vrijednosti uzrokovanih kibernetičkim napadom).

Visok rizik predstavlja i kineski plan za integraciju digitalnih sektora telekomunikacija (uključujući velike tvrtke ZTE, China Mobile i Huawei), IoT-a i e-trgovine (kineske tvrtke Alibaba i JD.com) za stvaranje regionalne povezanosti. Plan predviđa tehnološki poredak temeljen na kineskom izvozu digitalne infrastrukture kao što su prekogranični optički kabeli i druge komunikacijske mreže kojima bi se prikupljale velike količine podataka [60].

6.4 Mjere za ublažavanje rizika

Prije implementacije uređaje treba sigurnosno testirati. Kupci bi trebali inzistirati na dodacima u ugovorima s dobavljačima koji im omogućuju provođenje neovisnih sigurnosnih testiranja svakog uređaja i pripadajućih sigurnosnih ažuriranja te izvještavanje dobavljača o rezultatima testiranja [71].

Prilikom testiranja potrebno je uključiti hardverske i softverske komponente svakog uređaja, uključujući:

• podatke koje uređaj prikuplja,

• mrežna sučelja (*Ethernet*, WiFi, *Bluetooth* itd.),

• izloženost internetu,

• fizičku lokaciju (podatkovni centar, bazna stanica itd.),

• fizička sučelja,

• softverske ranjivosti,

• bibliotečne ranjivosti,

• ranjivosti konfiguracije,

• zadane vjerodajnice [71].

Nadalje, u mreži treba koristiti opremu više dobavljača i izbjegavati visokorizičnu opremu u kritičnim dijelovima mreže.

Jedan od načina kojim Huawei nastoji sigurnost opreme učiniti transparentnom su sigurnosni centri. U Banbury-ju, Oxfordshire je 2010. otvoren *The UK Huawei Cyber Security Evaluation Centre* s ciljem ublažavanja svih uočenih rizika koji proizlaze iz uključenosti Huaweija u dijelove

kritične nacionalne infrastrukture Ujedinjenog Kraljevstva. Centar ima pristup izvornom kôdu tih uređaja te može provesti reviziju i opsežna testiranja svoje opreme [71].

7. Napori Europske unije u ostvarenju i očuvanju sigurnosti 5G mreže

5G mreže će digitalno transformirati društvo i gospodarstvo EU-a. Kibernetička sigurnost 5G mreža ključna je za zaštitu našeg gospodarstva i društva te za ostvarenje punog potencijala mogućnosti koje 5G nudi kao i za stratešku autonomiju EU-a [3].

U ovom poglavlju opisane su radnje koje se poduzimaju u EU-u i predstavljene mjere kojima se nastoji osigurati sigurnost 5G mreže svih njenih država članica.

7.1 Koordinirana procjena rizika sigurnosti 5G mreža na razini Europske unije

Europska komisija je od svih svojih država članica u ožujku 2019. zatražila provedbu nacionalne procjene rizika 5G mrežne infrastrukture. U srpnju iste godine procjene rizika su dostavljene Komisiji i Agenciji Europske unije za kibernetičku sigurnost (engl. *The European Union Agency for Cybersecurity*, ENISA). Pristup procjeni rizika modeliran je na temelju pretpostavki o slučajevima uporabe i mogućim scenarijima. Na temelju dobivenih procjena objavljen je izvještaj koji identificira glavne prijetnje i aktere prijetnji, najosjetljiviju imovinu, glavne ranjivosti te glavne povezane rizike [73]. U Republici Hrvatskoj je procjenu rizika koordinirala Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM) [74].

U izvješću su istaknuti sigurnosni izazovi povezani sa:

- rastućom brigom o sigurnosti koja se tiče zaštite dostupnosti i cjelovitosti mreže te povjerljivosti i privatnosti podataka,
- ključnim inovacijama u 5G tehnologiji, osobito povećanom ulogom softvera i širokim rasponom usluga i aplikacija koje 5G mreže omogućuju,
- ulogom dobavljača u izgradnji i radu 5G mreža, složenošću veza između dobavljača i operatora te stupnjem ovisnosti o pojedinom dobavljaču [3].

Utvrđeno je da se najveći broj prijetnji odnosi na:

- prekid lokalne ili globalne 5G mreže - ugrožena dostupnost,
- špijuniranje prometa/podataka u 5G mrežnoj infrastrukturi - ugrožena povjerljivost,
- izmjena ili preusmjeravanje prometa/podataka u 5G mrežnoj infrastrukturi - ugrožena cjelovitost i/ili povjerljivost,
- uništavanje ili izmjena drugih digitalnih infrastruktura ili informacijskih sustava putem 5G mreža - ugrožena cjelovitost i/ili dostupnost [73].

Ozbiljnost prijetnji na 5G mreže može varirati ovisno o brojnim čimbenicima, osobito o:

- broju i vrsti korisnika na koje prijetnja utječe,
- vremenu trajanja događaja prije otkrivanja ili sanacije,
- vrsti usluga na koje prijetnja utječe (javna sigurnost, hitne službe, zdravlje, vladine aktivnosti, električna energija, voda itd.), opsegu štete ili ekonomskim gubicima,

- vrsti informacije koja je ugrožena [73].

Relevantnost aktera prijetnje procijenjena je kombiniranjem dva parametra: procjenom njihovih sposobnosti (resursa) te njihove namjere u provođenju ili pokušaju provođenja napada na 5G mrežnu infrastrukturu (motivacija). Utvrđeno je da su prijetnje od strane države ili sponzorirane od države od najveće važnosti i mogu uzrokovati velike prekide ili značajne smetnje u telekomunikacijskim uslugama iskorištavanjem nedokumentiranih funkcija ili napadom na kritičnu infrastrukturu poput opskrbe električnom energijom. Također se napominje da se napadači iznutra ili podizvođači u određenim okolnostima također mogu smatrati potencijalnim akterima prijetnje, osobito ako ih države iskoriste kao kanal za pristup kritičnoj ciljanoj imovini [73]. Na Slika 7.1 su prikazane kategorije prijetnje i akteri prijetnji.

Slika 7.1 Procjena rizika kibernetičke sigurnosti 5G mreže država članica EU-a – kategorije prijetnje i akteri prijetnji [73]

Kod procjene osjetljivosti mrežne opreme u obzir su uzeti sljedeći kriteriji:

- vrsta utjecaja, npr. uzrokuje li ostvarenje prijetnje narušavanje povjerljivosti i/ili dostupnosti i/ili cjelovitosti mreže,
- razmjer utjecaja, npr. u pogledu korisnika, trajanja, broja zahvaćenih baznih stanica, osjetljivosti promijenjenih ili dohvaćenih informacija [73].

Tablica 7.1 prikazuje glavne kategorije elemenata i funkcija, njihovu ukupnu razinu osjetljivosti te niz ključnih elemenata za svaku kategoriju.

Tablica 7.1 Procjena rizika kibernetičke sigurnosti 5G mreže država članica EU-a - popis i klasifikacija mrežnih funkcija i ključnih elemenata [73]

Kategorije elemenata i funkcija		**Primjeri ključnih elemenata**
Funkcije jezgrene mreže	**KRITIČNA**	Funkcije provjere autentifikacije korisničke opreme, roaminga i upravljanja sjednicama
		Funkcije prijenosa podataka korisničke opreme
		Registracija i autorizacija mrežnih usluga
		Pohrana podataka krajnjih korisnika i mrežnih podataka
		Veza s mobilnim mrežama trećih strana
		Izlaganje funkcija jezgrene mreže vanjskim aplikacijama
		Pripisivanje uređaja krajnjih korisnika mrežnim dijelovima
Upravljanje NFV-om i orkestracija mreže (MANO)	**KRITIČNA**	
Sustavi upravljanja i usluge podrške (osim MANO-a)	**UMJERENA/VISOKA**	Sustavi upravljanja sigurnošću
		Naplata i drugi sustavi podrške
Radio pristupna mreža	**VISOKA**	Bazne stanice
Transportne i prijenosne funkcije	**UMJERENA/VISOKA**	Mrežna oprema niske razine (usmjernici, preklopnici itd.)
		Mrežna oprema za filtriranje prometa (vatrozidi, IPS itd.)
Razmjene među mrežama	**UMJERENA/VISOKA**	Mrežne usluge koje pružaju treće strane

U izvješću su države članice procijenile tri vrste ranjivosti: ranjivosti vezane za hardver, softver, procese i politike, ranjivosti specifične za dobavljača i ranjivosti proizišle iz ovisnosti o pojedinom dobavljaču.

5G mreže se u velikoj mjeri temelje na softveru. Veliki sigurnosni propusti poput onih koji proizlaze iz loših procesa razvoja softvera dobavljača opreme mogu olakšati zlonamjerno umetanje i zlouporabu stražnjih vrata u proizvode i otežati njihovo otkrivanje. Potrebno je istaknuti nedostatak ili neodgovarajuće procedure sigurnosnog ili operativnog održavanja poput ažuriranja softvera/upravljanja zakrpama. Ta će ranjivost postati puno izraženija u 5G mrežama zbog veće

učestalosti održavanja i ažuriranja sustava kojim se nastoji smanjiti izloženost mreže sigurnosnim rizicima [73].

Povećana uloga softvera i usluga koje pružaju dobavljači trećih strana dovodi do veće izloženosti brojnim ranjivostima koje mogu proizaći iz profila rizika pojedinih dobavljača. Profili rizika pojedinih dobavljača mogu se procijeniti na temelju nekoliko čimbenika:

- vjerojatnost utjecaja trećih zemalja na dobavljača što je jedan od ključnih aspekata u procjeni netehničkih ranjivosti 5G mreža. Taj utjecaj može uključivati:
  - snažnu vezu između dobavljača i vlade određene treće zemlje,
  - zakonodavstvo treće zemlje, osobito ako ne postoje zakonodavne ili demokratske kontrole i ravnoteže ili nedostatak sporazuma o sigurnosti ili zaštiti podataka između EU-a i treće zemlje,
  - karakteristike korporacijskog vlasništva dobavljača,
  - mogućnost da treća zemlja provodi bilo kakav oblik pritiska, uključujući i mjesto proizvodnje opreme.
- sposobnost dobavljača da osigura opskrbu,
- cjelokupna kvaliteta proizvoda i prakse kibernetičke sigurnosti dobavljača uključujući stupanj kontrole nad vlastitim opskrbnim lancem i prisutnost prioritizacije sigurnosnih praksi [73].

Značajne ranjivosti proizlaze iz nedostatka raznolikosti u korištenju opreme i rješenja, kako unutar pojedinačnih mreža, tako i na nacionalnoj razini. Oslanjanje na jednog dobavljača unutar pojedinačnih mreža stvara ovisnost o specifičnim rješenjima i otežava nabavu rješenja od drugih dobavljača, posebno gdje rješenja nisu u potpunosti interoperabilna. Na nacionalnoj razini i razini EU-a nedostatak raznolikosti dobavljača povećava ukupnu ranjivost 5G infrastrukture, posebno ako velik broj operatora svoju osjetljivu imovinu nabavlja od dobavljača koji predstavlja visok stupanj rizika, tj. visokorizičnog dobavljača [73]**.**

Provedenim procjenama rizika unutar EU-a identificirano je nekoliko kategorija glavnih sigurnosnih rizika i scenarija rizika koji opisuju moguće vrste napada (Tablica 7.2) [3].

Tablica 7.2 Procjena rizika kibernetičke sigurnosti 5G mreže država članica EU-a - kategorije i scenariji glavnih rizika [3]

I - Scenariji rizika povezani s nedovoljnim mjerama sigurnosti	**R1** - Pogrešna konfiguracija mreže: zbog loše konfiguriranog sustava i arhitekture državni akter putem vanjskih sučelja može prodrijeti u 5G mrežu što ugrožava funkcije jezgrene mreže ili iskorištava čvorove rubnog računarstva s namjerom narušavanja povjerljivosti informacija i distribuiranih usluga. **R2** - Nedostatak kontrola pristupa: podizvođač s administratorskim ovlastima obavlja zlonamjerne radnje što dovodi do narušavanja povjerljivosti/cjelovitosti i/ili dostupnosti 5G mreže i/ili usluga. Radnje podizvođača mogu biti posljedica nametnutog zakonskog zahtjeva.

II - Scenariji rizika povezani s opskrbnim lancem	**R3** - Niska kvaliteta proizvoda: špijunaža zlonamjernim programom od strane države ili sponzorirana od države u svrhu zlouporabe ranjivih mrežnih komponenti ili ranjivosti koje utječu na osjetljive elemente u jezgrenoj mreži kao što su funkcije mrežne virtualizacije. **R4** - Ovisnost o bilo kojem pojedinačnom dobavljaču unutar pojedinačnih mreža ili nedostatak raznolikosti dobavljača na nacionalnoj razini: operator veliku količinu svojih osjetljivih mrežnih komponenti ili usluga nabavlja od jednog dobavljača. Dostupnost opreme i/ili zakrpi tog dobavljača se naknadno drastično smanjuje zbog problema u opskrbi (npr. zbog trgovinskih sankcija treće zemlje ili drugih komercijalnih okolnosti). Posljedično, kvaliteta opreme dobavljača opada zbog prioriteta koji se daje jamčenju opskrbe nad poboljšanjima u sigurnosti proizvoda.
III - Scenariji rizika povezani s načinom rada aktera prijetnje	**R5 -** Uplitanje države u 5G lanac opskrbe: neprijateljski državni akter vrši pritisak na dobavljača pod svojom jurisdikcijom u svrhu pristupa osjetljivoj mrežnoj opremi kroz namjerno ili nenamjerno ugrađene ranjivosti. **R6** - Iskorištavanje 5G mreža od strane organiziranog kriminala ili organizirane kriminalne grupe koja cilja krajnje korisnike: preuzimanjem kontrole nad kritičnim dijelom 5G mrežne arhitekture organizirana kriminalna grupa ometa razne usluge kako bi ucijenila tvrtke koje se oslanjaju na te usluge ili samog operatora. Organizirana kriminalna grupa korištenjem sličnog vektora napada može ciljati krajnje korisnike *phishing* kampanjom, online prijevarama ili korištenjem kompromitirane mreže za pristup povjerljivim podacima o korisnicima radi daljnje zarade.
IV - Scenariji rizika koji se odnose na međuovisnost 5G mreža i drugih kritičnih sustava	**R7** - Značajan prekid u radu kritične infrastrukture ili usluga: zlonamjerni hakeri mogu ugroziti hitne službe preuzimanjem kontrole nad dodijeljenim mrežnim dijelom čime ugrožavaju dostupnost usluge i cjelovitost informacija/podataka koji se koriste za/unutar te usluge. **R8** - Masivni kvar mreža zbog prekida opskrbe električnom energijom ili drugih sustava podrške: masovni prekid napajanja električnom energijom zbog prirodnih katastrofa ili napada na energetsku mrežu od strane države/sponzorirane od države ili organizirane kriminalne grupe.
V - Scenariji rizika povezani s uređajima krajnjih korisnika	**R9** - Iskorištavanje IoT-a: grupa haktivista ili akter sponzoriran od države preuzima kontrolu nad uređajima s niskom razinom sigurnosti poput IoT-a (senzori,

	kućanski aparati itd.) s namjerom napada na mrežu preplavljivanjem signalizacijske ravnine.

Procijenjene rizike je nužno ublažiti što se preporuča mjerama navedenim u EU Toolboxu objavljenom 29. siječnja 2020.

7.2 Alat za ublažavanje rizika na razini Europske unije

Ciljevi EU Toolboxa (dalje u tekstu: alat) su identificirati zajednički skup mjera koje mogu ublažiti procijenjene glavne rizike kibernetičke sigurnosti 5G mreža te dati smjernice za odabir prioritetnih mjera u planovima ublažavanja rizika na nacionalnoj razini i razini EU-a. Time se nastoje zaštiti povjerljivost, cjelovitost i dostupnost 5G mreža kroz:

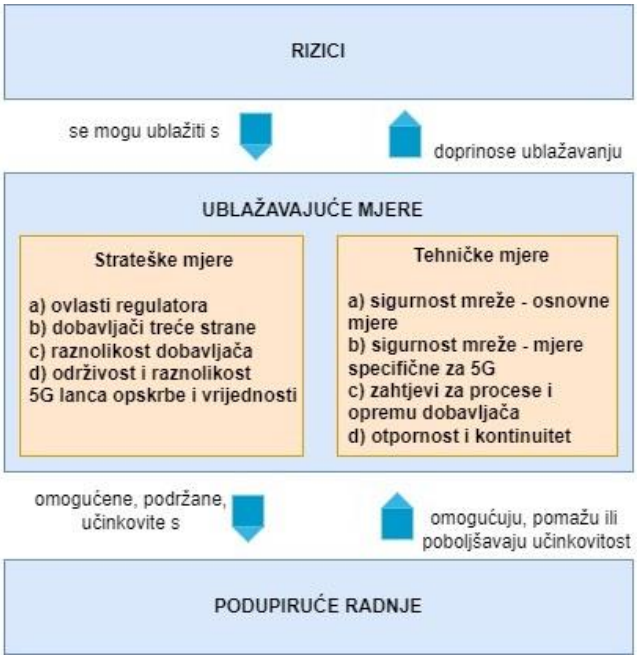
- jačanje sigurnosti u projektiranju, upogonjavanju i radu mreža,
- podizanje osnovnih standarda sigurnosti za sigurnost proizvoda i usluga,
- minimiziranje izloženosti rizicima koji proizlaze iz profila rizika pojedinog dobavljača,
- izbjegavanje ili ograničavanje velikih ovisnosti o bilo kojem pojedinačnom dobavljaču 5G mrežne opreme i usluga,
- promicanje raznolikog, konkurentnog i održivog tržišta 5G opreme i usluga uključujući i održavanje europskih kapaciteta u 5G lancu vrijednosti [3].

Alat je podijeljen na 8 strateških i 11 tehničkih mjera te 10 podupirućih radnji kako je prikazano na Slika 7.2. Mjere se tiču relevantnih sudionika sigurnosti u 5G sustavu, prvenstveno operatora i njihovih dobavljača telekomunikacijske opreme.

Strateške mjere obuhvaćaju mjere kojima regulatorna i druga nacionalna tijela mogu pojačano nadzirati nabavu i upogonjavanje mrežne opreme, mjere za rješavanje rizika povezanih s netehničkim ranjivostima (npr. rizik od uplitanja treće zemlje ili rizik od ovisnosti o jednom dobavljaču) kao i moguće inicijative za promicanje održivog i raznolikog lanca opskrbe 5G mreže:

- SM01: jačanje uloge nacionalnih tijela,
- SM02: provođenje revizije nad operatorima i zahtijevanje informacija od operatora,
- SM03: procjena profila rizika dobavljača i primjena ograničenja na visokorizične dobavljače - uključujući potrebna isključenja za učinkovito ublažavanje rizika - za ključnu imovinu,
- SM04: kontrola vanjskih pružatelja usluga (engl. *Managed Service Providers*, MSP) i podrške treće strane proizvođača opreme,
- SM05: osiguravanje raznolikosti dobavljača za pojedinačne operatore kroz odgovarajuće strategije za više dobavljača,
- SM06: jačanje otpornosti na nacionalnoj razini,
- SM07: identificiranje ključne imovine i njegovanje raznolikog i održivog 5G sustava u EU-u,

- SM08: održavanje i izgradnja raznolikosti i kapaciteta EU-a u budućim mrežnim tehnologijama [3].



Slika 7.2 Alat - mjere i podupiruće radnje za ublažavanje procijenjenih sigurnosnih rizika [3]

Tehničke mjere uključuju mjere za jačanje sigurnosti 5G mreže i opreme jačanjem sigurnosti tehnologija, procesa, ljudi i fizičkih čimbenika. Učinkovitost tehničkih mjera razlikovat će se ovisno o opsegu mjera i vrsti rizika koje treba ublažiti:

- TM01: osiguravanje primjene osnovnih sigurnosnih zahtjeva (siguran mrežni dizajn i arhitektura),
- TM02: osiguravanje i ocjena provedbe sigurnosnih mjera u postojećim 5G standardima,
- TM03: osiguravanje strogih kontrola pristupa,
- TM04: povećavanje sigurnosti funkcija virtualne mreže,
- TM05: osiguravanje sigurnog upravljanja, rada i nadzora 5G mreže,
- TM06: jačanje fizičke sigurnosti,
- TM07: jačanje cjelovitosti softvera, ažuriranja i upravljanja zakrpama,
- TM08: podizanje sigurnosnih standarda u dobavljačkim procesima pomoću strogih uvjeta nabave,
- TM09: korištenje europskih certifikata za mrežne komponente, korisničku opremu i/ili procese dobavljača 5G mreže,
- TM10: korištenje europskih certifikata za druge proizvode i usluge informacijske i komunikacijske tehnologije koje nisu specifične za 5G (povezani uređaji, usluge u oblaku),
- TM11: jačanje planova otpornosti i kontinuiteta [3].

Podupiruće radnje mogu povećati učinkovitost strateških i tehničkih mjera:

- SA01: pregled ili razvoj smjernica i najboljih praksi za sigurnost mreže,
- SA02: jačanje sposobnosti ispitivanja i revizije na nacionalnoj i EU razini,
- SA03: podrška i oblikovanje 5G standardizacije,
- SA04: razvoj smjernica za provedbu sigurnosnih mjera u postojećim 5G standardima,
- SA05: osiguravanje primjene standardnih tehničkih i organizacijskih sigurnosnih mjera putem posebne sheme certificiranja na razini EU-a,
- SA06: razmjena najboljih praksi u provedbi strateških mjera, posebno nacionalnih okvira za procjenu profila rizika dobavljača,
- SA07: poboljšanje koordinacije prilikom odgovora na incidente i upravljanja krizama,
- SA08: provođenje revizija međuovisnosti 5G mreža i drugih kritičnih usluga,
- SA09: jačanje mehanizama suradnje, koordinacije i razmjene informacija,
- SA10: uzimanje kibernetičkih sigurnosnih rizika u obzir kod upogonjavanja 5G projekata podržanih javnim sredstvima [3].

Provedba strateških mjera može zahtijevati uvođenje novih zakona na nacionalnoj razini kako bi se u potpunosti postigao njihov učinak. Neke su države članice EU-a već prilagodile svoje zakonodavstvo strateškim mjerama dok su druge u procesu izmjene postojećih ili donošenja novih zakona.

U Republici Hrvatskoj je oformljena nacionalna radna skupina koju koordinira HAKOM. Zadaća skupine je odabrati mjere iz alata i definirati kriterije za dobavljače opreme koji žele raditi u Hrvatskoj. Domaći operatori će 5G opremu i usluge moći nabaviti od proizvođača koji će zadovoljiti postavljene kriterije [74].

U nastavku rada opisane su strateške mjere (Tablica 7.3) i osma tehnička mjera (Tablica 7.4) budući se pomoću nekih od njih nastoji smanjiti negativna uloga dobavljača opreme u sigurnosti 5G mreže.

Tablica 7.3 Strateške mjere [3]

STRATEŠKE MJERE					
a) Regulatorne ovlasti					
Broj	Mjera	Opis	Povezani rizici	Povezani akteri	Podupiruće radnje
SM01	Jačanje uloge nacionalnih tijela	Mjera uključuje regulatorne ovlasti za nacionalna tijela kako bi: - nametnula pojačane obveze operatorima, npr. u dijelu sigurnosti signalizacijske/upravljačke ravnine - koristila *ex-ante* ovlasti za ograničavanje, zabranu i/ili nametanje posebnih zahtjeva ili uvjeta za opskrbu, implementaciju i rad 5G mrežne opreme, uzimajući u obzir: • sigurnost kritičnih i osjetljivih dijelova 5G mreža, • sigurnost same opreme ili okruženja (upogonjavanje, međusobno povezivanje itd.), • rizik od uplitanja treće zemlje u opskrbni lanac 5G opreme, • rizik od velike ovisnosti operatora ili države o pojedinačnom dobavljaču, • rizike za nacionalnu sigurnost.	R1 R2 R3 R4 R5 R6 R7	Relevantne vlasti Operatori	SA01 SA04 SA06
SM02	Provođenje revizije nad operatorima i zahtijevanje informacija	Prilikom vršenja svojih ovlasti prema članku 41. stavku 2. Europskog kodeksa elektroničkih komunikacija (engl. *European Electronic Communications Code*, EECC), nadležna tijela bi trebala: - provoditi reviziju ili zahtijevati provođenje revizija nad operatorima, ako je potrebno na dubinskoj tehničkoj razini, npr. kritičnih komponenti i/ili osjetljivih dijelova 5G mreža, - zahtijevati od operatora dostavu detaljnih i ažuriranih informacija o planovima nabave 5G opreme i o uključivanju dobavljača trećih strana, - zahtijevati od operatora dokumentiranje i održavanje opisa o provedbi osnovnih tehničkih mrežnih sigurnosnih mjera.	R1 R2 R3 R4 R5 R6 R7	Relevantne vlasti Operatori	SA02
b) Dobavljači trećih strana					
SM03	Procjena profila rizika dobavljača i primjena	Uspostaviti okvir s jasnim kriterijima (uzimajući u obzir čimbenike rizika utvrđene u stavku 2.37 koordiniranog izvješća o procjeni rizika u EU-u [73] i podatke specifične za svaku državu poput procjene prijetnji od	R2 R5	Relevantne vlasti Operatori	SA06 SA10

	ograničenja na one dobavljače koji se smatraju visokorizičnima - uključujući potrebna isključenja za učinkovito ublažavanje rizika - za ključnu imovinu	strane nacionalnih sigurnosnih službi) na temelju kojeg će nacionalna nadležna tijela i operatori: - provoditi rigorozne procjene profila rizika svih relevantnih dobavljača na nacionalnoj i/ili EU razini (primjerice, zajedno s drugim državama članicama EU-a ili drugim operatorima), - na temelju procjene profila rizika, primijeniti ograničenja, uključujući potrebna isključenja za učinkovito ublažavanje rizika, za ključnu imovinu definiranu kao kritičnu ili osjetljivu u koordiniranom izvješću o procjeni rizika (funkcije jezgrene mreže, funkcije upravljanja i orkestracije mreže te funkcije pristupa mreži), - poduzeti korake na temelju kojih će operatori provoditi odgovarajuće kontrole i procese za upravljanje potencijalnim preostalim rizicima poput redovite revizije lanca opskrbe i procjene rizika, robusnog upravljanja rizikom i/ili posebnih zahtjeva za dobavljače na temelju njihovog profila rizika.			
SM04	Kontrola MSP-ova i podrške treće strane dobavljača opreme	Uspostaviti pravni/regulatorni okvir koji ograničava aktivnosti i uvjete pod kojima operatori određene funkcije mogu povjeriti MSP-ovima kako za fizičku tako i za virtualnu infrastrukturu, uključujući: - primjenu ograničenja, posebno u osjetljivim dijelovima 5G mreža poput sigurnosnih i mrežnih operativnih funkcija i gdje se MSP-ovi smatraju visokorizičnim dobavljačima po mjeri SM03, - nametanje pojačanih sigurnosnih odredbi koje se odnose na pristup koji MSP-ovi imaju za obavljanje povjerenih im funkcija, - nametanje strogih kontrola pristupa podršci treće strane proizvođača opreme tijekom projektiranja, upogonjavanja i/ili rada mreže, posebno kritično osjetljivim komponentama i/ili osjetljivim dijelovima mreže te posebno za dobavljače koji se smatraju visokorizičnim dobavljačima po mjeri SM03.	R2 R5	Relevantne vlasti Operatori	SA06 SA10
c) Raznolikost dobavljača					
SM05	Osiguravanje raznolikosti dobavljača za pojedinačne operatore kroz odgovarajuće	Osigurati da svaki operator ima odgovarajuću strategiju za više dobavljača uzimajući u obzir tehnička ograničenja i zahtjeve interoperabilnosti različitih dijelova 5G mreže: - kako bi se izbjegla ili ograničila bilo kakva veća ovisnost o jednom dobavljaču ili dobavljačima sa sličnim profilom rizika,	R4	Relevantne vlasti Operatori	SA03 SA10

	strategije za više dobavljača	- kako bi se izbjegla ovisnost o visokorizičnim dobavljačima sukladno mjeri SM03.			
SM06	Jačanje otpornosti na nacionalnoj razini	Osigurati odgovarajuću ravnotežu dobavljača na nacionalnoj razini kako bi se osigurala otpornost u slučaju incidenta s jednim operatorom i/ili jednim dobavljačem, uzimajući u obzir varijacije u zemljopisnom položaju i broju stanovnika u pojedinim državama članicama.	R4	Relevantne vlasti Operatori	SA03 SA10
d) Održivost i raznolikost 5G lanca opskrbe i vrijednosti					
SM07	Identificiranje ključne imovine i njegovanje raznolikog i održivog 5G sustava u EU-u	Nadograditi europski mehanizam provjeravanja izravnih stranih ulaganja radi poboljšanja praćenja izravnih stranih ulaganja u 5G lancu vrijednosti (npr. mapiranjem ključne 5G imovine, upotrebom alata za praćenje i istraživanjem posebnih smjernica) kako bi se lakše otkrile strane investicije koje mogu predstavljati prijetnju na sigurnost ili javni red u državama članicama EU-a. Kritična infrastruktura, javna sigurnost, pristup informacijama, kontrola informacija i kibernetička sigurnost dobro su ugrađeni u opseg primjene uredbe o direktnim stranim ulaganjima, dopuštajući procjenu ulaganja, uzimajući u obzir čimbenike poput profila rizika kupaca/tvrtki.	R4	Europska komisija i države članice EU-a	SA10
SM08	Održavanje i izgradnja raznolikosti i kapaciteta EU-a u budućim mrežnim tehnologijama	Razviti politike koje stvaraju optimalne uvjete za europske tehnološke tvrtke i poticati inovacije u ključnim tehnološkim područjima za promicanje raznolikog, održivog i sigurnog europskog 5G sustava, uključujući: - razvoj predloženog europskog institucionaliziranog partnerstva u području Interneta sljedeće generacije/6G ("Pametne mreže i usluge", program *Horizon Europe*) kako bi se osigurao dovoljan stupanj raznolikosti dobavljača i dovoljno znanja i kapaciteta opskrbe u EU-u duž cijelog lanca vrijednosti telekomunikacija, - razvoj europskih kapaciteta EU-a podržavanjem ambicioznih istraživanja i inovacija čime se izbjegavaju ovisnosti. To se odnosi na provedbu različitih europskih programa financiranja, osobito *Horizon Europe*, *Digital Europe Programme* i *Connecting Europe Facility* (CEF), - okupljanje znanja, stručnosti, financijskih sredstava i gospodarskih aktera diljem EU-a radi prevladavanja potencijalnih važnih tržišnih ili sustavnih propusta duž lanca vrijednosti te daljnje specifične industrijske inicijative.	R4	Europska komisija i države članice EU-a Svi 5G sudionici	SA10

Tablica 7.4 Osma tehnička mjera [3]

TEHNIČKA MJERA					
Zahtjevi vezani za procese i opremu dobavljača					
Broj	Mjera	Opis	Povezani rizici	Povezani akteri	Podupiruće radnje
TM08	Podizanje sigurnosnih standarda u procesima dobavljača kroz stroge uvjete nabave	Osigurati da operatori od dobavljača opreme zahtijevaju posebne sigurnosne standarde u postupku nabave (npr. specifična sigurnosna poboljšanja i dokazivanje razine kvalitete, sigurnosno održavanje opreme tijekom njezina vijeka trajanja i ugrađena sigurnost u razvojnim procesima proizvoda).	R3 R6 R7	Relevantne vlasti Operatori Dobavljači	SA02 SA10

S obzirom na širok raspon područja rizika identificiranih u europskoj koordiniranoj procjeni rizika i njihovu različitu prirodu, jedna mjera za njihovo ublažavanje nije dovoljna, već niz prikladnih mjera za rješavanje svih ključnih područja rizika. Na temelju procjene mogućih planova ublažavanja i utvrđivanja najučinkovitijih mjera ovaj alat preporučuje:

1. Sve države članice EU-a bi trebale uspostaviti mjere (uključujući ovlasti za nacionalna tijela) kao odgovor na trenutno identificirane i buduće rizike. Nadalje, trebaju ograničiti, zabraniti i/ili nametnuti posebne zahtjeve ili uvjete, prema pristupu temeljenom na riziku, u opskrbi, upogonjavanju i radu 5G mrežne opreme na temelju niza sigurnosnih osnova. Posebno bi trebale:
   - nametati sigurnosne zahtjeve operatorima (npr. stroge kontrole pristupa, pravila o sigurnom radu i praćenju, ograničiti povjeravanje određenih funkcija vanjskim podizvođačima itd.),
   - procijeniti profil rizika dobavljača i primijeniti odgovarajuća ograničenja za visokorizične dobavljače, uključujući potrebna isključenja za učinkovito ublažavanje rizika za ključnu imovinu definiranu kao kritičnu i osjetljivu (npr. pristupne mrežne funkcije, funkcije jezgrene mreže, funkcije upravljanja i orkestracije mreže),
   - osigurati da svaki operator ima odgovarajuću strategiju za više dobavljača kako bi se izbjegla ili ograničila bilo kakva velika ovisnost o jednom dobavljaču (ili dobavljačima sa sličnim profilom rizika), osigurati odgovarajuću ravnotežu dobavljača na nacionalnoj razini i izbjeći ovisnost o visokorizičnim dobavljačima što također zahtijeva izbjegavanje zaključavanja nabava na jednog dobavljača, uključujući i promicanje veće interoperabilnosti opreme [3].

2. Europska komisija bi s državama članicama trebala pridonijeti:

   - održavanju raznolikog i održivog 5G lanca opskrbe kako bi se izbjegla dugoročna ovisnost, uključujući:
     - potpuno korištenje postojećih europskih alata i instrumenata osobito provjeravanjem potencijalnih izravnih stranih ulaganja koji utječu na ključnu 5G imovinu te izbjegavanje poremećaja na tržištu 5G opskrbe koji proizlaze iz potencijalnih subvencija ili spuštanja cijena ispod cijene proizvodnje,
     - daljnje jačanje europskih kapaciteta u 5G i *post*-5G tehnologijama korištenjem odgovarajućih europskih programa i financiranja.
   - jačanju koordinacije između država članica u pogledu standardizacije radi postizanja posebnih sigurnosnih ciljeva i razvoj relevantnih shema certificiranja na europskoj razini radi promicanja sigurnijih proizvoda i procesa [3].

3. Potrebno je proširiti grupu *The Network and Information Systems Cooperation Group Stream* (NIS) i suradnju s drugim relevantnim tijelima i subjektima radi:

   - povremenog revidiranja nacionalne i europske procjene rizika o sigurnosti 5G i *post*-5G mreža dodatno razrađujući i usklađujući buduću metodologiju procjene i prilagođavajući se razvijajućoj 5G tehnologiji,

- detaljnog i redovitog praćenja te evaluacije provedbe alata na temelju strukturiranih izvješća država članica EU-a,
- koordinacije i podrške provedbi podupirućih radnji koje zahtijevaju suradnju na europskoj razini, posebno u pogledu izrade smjernica i razmjene najboljih praksi o različitim mjerama,
- podrške daljnje koordinacije na europskoj razini osobito zbog postizanja daljnje konvergencije u tehničkim i organizacijskim sigurnosnim zahtjevima za operatore [3].

7.3 Praška konferencija o 5G sigurnosti

U Pragu je 3. svibnja 2019. održana konferencija o 5G sigurnosti na kojoj su dani prijedlozi za uvođenje 5G-a i budućih mobilnih mreža. Prijedlozi su podijeljeni u četiri kategorije: politika, tehnologija, ekonomija te sigurnost, privatnost i otpornost [75].

1. Politika:

- Komunikacijske mreže i usluge treba projektirati na način da budu otporne i sigurne. Mreže treba izgraditi i održavati koristeći najbolju praksu o kibernetičkoj sigurnosti temeljene na riziku te međunarodne, otvorene standarde zasnovane na konsenzusu. Treba promicati jasne globalno interoperabilne smjernice o kibernetičkoj sigurnosti koje bi podržale kibernetičke sigurnosne proizvode i usluge u jačanju otpornosti svih sudionika.
- Svaka je država slobodna, u skladu s međunarodnim pravom, postaviti vlastite zahtjeve za nacionalnu sigurnost i provedbu zakona koji bi trebali poštivati privatnost i pridržavati se zakona koji štite informacije od nepropisnog prikupljanja i zlouporabe.
- Zakoni i politike koji uređuju mreže i usluge povezivanja trebali bi se voditi načelima transparentnosti i pravičnosti, uzimajući u obzir globalno gospodarstvo i interoperabilna pravila, uz dovoljan nadzor i poštivanje vladavine prava.
- Treba uzeti u obzir rizik utjecaja treće zemlje na dobavljača, osobito u odnosu na njen model upravljanja, nepostojanje ugovora o suradnji na području sigurnosti ili sličnih sporazuma, poput odluka o primjerenosti u pogledu zaštite podataka [75].

2. Tehnologija:

- Sudionici bi trebali redovito provoditi procjene ranjivosti i ublažavanje rizika u svim komponentama i mrežnim sustavima prije objavljivanja proizvoda i tijekom rada sustava te provoditi pravovremena ažuriranja i nadogradnje radi ublažavanja identificiranih ranjivosti.
- Procjene rizika proizvoda dobavljača trebale bi uzeti u obzir sve relevantne čimbenike, uključujući primjenjivo pravno okruženje i druge aspekte dobavljačevog ekosustava jer ti čimbenici mogu biti bitni za napore sudionika u zadržavanju najviše moguće razine kibernetičke sigurnosti.
- Prilikom izgradnje otpornosti i sigurnosti treba uzeti u obzir činjenicu kako zlonamjerne kibernetičke aktivnosti ne zahtijevaju uvijek iskorištavanje tehničke ranjivosti kao npr. u slučaju napada iznutra.

- Radi povećanja koristi od globalne komunikacije, države članice EU-a bi trebale usvojiti politike koje će omogućiti učinkovit i siguran protok mrežnih podataka.
- Sudionici bi trebali uzeti u obzir tehnološke promjene koje prate uvođenje 5G mreža (npr. MEC, SDN, NFV) te njihov utjecaj na ukupnu sigurnost komunikacijskih kanala.
- Kupac (vlada, operator ili proizvođač) mora moći dobiti informaciju o izvornosti i podrijetlu komponenti i softvera koji utječu na razinu sigurnosti proizvoda ili usluge, u skladu s najnovijim dostignućima i odgovarajućim komercijalnim i tehničkim praksama, uključujući transparentnost održavanja, ažuriranja i popravaka proizvoda i usluga [75].

3. Ekonomija:

- Raznoliko i živo tržište komunikacijske opreme i lanac opskrbe ključni su za sigurnost i gospodarsku otpornost.
- Snažna ulaganja u istraživanje i razvoj pogoduju globalnom gospodarstvu i tehnološkom napretku te su način za potencijalno povećanje raznolikosti tehnoloških rješenja s pozitivnim učincima na sigurnost komunikacijskih mreža.
- Komunikacijske mreže i mrežne usluge bi se trebale otvoreno i transparentno financirati primjenom standardnih najboljih praksi u procesima nabave, ulaganja i ugovaranja.
- Poticaji, subvencije ili financiranje 5G mreža i pružatelja usluga koje sponzorira država trebaju poštivati načela pravičnosti, biti komercijalno razumni, provoditi se otvoreno i transparentno, na temelju načela tržišnog natjecanja, uzimajući u obzir trgovačke obveze.
- Važan je učinkovit nadzor nad ključnim financijskim i investicijskim instrumentima koji utječu na razvoj telekomunikacijske mreže.
- Komunikacijske mreže i pružatelji mrežnih usluga trebali bi imati transparentno vlasništvo, partnerstva i strukture korporativnog upravljanja [75].

4. Sigurnost, privatnost i otpornost:

- Svi sudionici, uključujući industriju, trebali bi zajedno raditi na promicanju sigurnosti i otpornosti nacionalnih kritičnih infrastrukturnih mreža, sustava i povezanih uređaja.
- Treba promicati razmjenu iskustva i najboljih praksi, uključujući, prema potrebi, pomoć u ublažavanju, istrazi, odgovoru i oporavku od mrežnih napada, nagodbi ili prekida.
- Sigurnost i procjene rizika dobavljača i mrežnih tehnologija trebaju uzeti u obzir vladavinu prava, sigurnosno okruženje, malverzacije dobavljača i usklađenost s otvorenim, interoperabilnim, sigurnim standardima i najboljim praksama u industriji za promicanje snažne i robusne kibernetičke sigurnosne opskrbe proizvoda i usluga radi suočavanja s rastućim izazovima.
- Treba implementirati okvir za upravljanje rizicima koji poštuje načela zaštite podataka kako bi se osigurala privatnost građana prilikom korištenja mrežne opreme i usluga [75].

8. Zaključak

Svaka nova generacija mobilnih mreža donosi nove prijetnje, rizike i ugrozu sigurnosti podataka koji se prenose mrežom. Ostvarenje kibernetičke sigurnosti 5G mreže je izazovno zbog puno veće količine osjetljivih podataka koje će prenositi, usluga koje će mrežu koristiti, prava pristupa dobavljača i trećih strana kako fizičkoj opremi tako i softveru, procedura ažuriranja softverskih inačica i nadzora mreže.

Dobavljači 5G opreme iz trećih zemalja, posebice Kine su pod posebnim povećalom zbog straha od kibernetičkih napada i prikupljanja/prisluškivanja podataka putem mogućih instaliranih stražnjih vrata u njihovoj opremi. To posljedično može uzrokovati krađu intelektualnog vlasništva, osobnih podataka, ali i izazvati kibernetičku krizu. Utjecaj vlasti na tvrtke u Kini je vidljiv iz donesenih zakona kojima vlada može provesti nadzor u tvrtkama te tražiti bezuvjetno ustupanje podataka u slučaju istrage o špijunaži. Nadalje, zakonom za tvrtke je propisano osnivanje organizacije Komunističke partije Kine za obavljanje djelatnosti stranke u skladu sa statutom Komunističke partije Kine.

Svi sudionici u 5G lancu su odgovorni za sigurnost 5G mreže te je njihova suradnja od velike važnosti: dobavljači opreme, operatori, pružatelji usluga, industrijski i državni regulatori. Operatori su odgovorni za kibernetičku otpornost 5G mreža te bi od dobavljača opreme trebali zahtijevati dokaze o strogoj kontroli kibernetičke sigurnosti lanca opskrbe i usklađenosti s načelima najbolje prakse u industriji ili relevantnim globalnim standardima. Operatori bi također trebali razmotriti zahtjev o usklađenosti s važećim standardima za kibernetičku sigurnost za operativnu sigurnost kao i kibernetičke sigurnosne certifikate ili sigurnosnu verifikaciju proizvoda (npr. NESAS). Dodatno, transparentnost vlasničke strukture dobavljača, ispitivanje izvornog kôda, odnosi s vladom i usklađenost sa zakonodavstvom su dio temelja povjerenja u dobavljače [49].

Sigurnost i neovisne revizije sigurnosti trebaju biti uključene u sve faze proizvodnje opreme: planiranje, razvoj, testiranje, implementacija i održavanje. Ukoliko oprema ima primjerice uvjerenje NESAS, ona zadovoljava listu sigurnosnih zahtjeva te je razvijena u skladu s razvojem dobavljača i procesima životnog ciklusa proizvoda koji pružaju sigurnost opreme.

Dobavljačima i partnerima bi se trebao zabraniti ili maksimalno ograničiti pristup opremi kao i softveru za upravljanje i nadzor mreže. Oprema bi trebala biti interoperabilna s opremom drugih dobavljača u slučaju potrebe za njenom zamjenom. Cijena ne smije biti presudni kriterij u nabavi opreme jer visokorizični dobavljači mogu ponuditi cijene ispod cijene proizvodnje zbog subvencija koje im pruža država.

Sigurnost 5G mreža u EU-u se nastoji ostvariti nizom mjera iz EU Toolboxa među kojima države članice trebaju primijeniti i nacionalno regulirati one koje mogu ublažiti procijenjene glavne rizike kibernetičke sigurnosti 5G mreži. Toolbox daje poseban naglasak na izbjegavanje uporabe opreme visokorizičnih dobavljača u ključnim dijelovima mreže te strategiju uporabe opreme više dobavljača.

5G mrežna tehnologija je kompleksna, velikim dijelom virtualizirana, temelji se na softveru, smještena je bliže korisniku i ranjivija je od prethodnih mobilnih generacija. Prijetnji na sigurnost 5G mreže je mnogo, od vandalizma nad fizičkom opremom do malicioznih napada presretanja i krađe podataka ili ažuriranja softvera s uključenim malicioznim kôdom. Prijetnju predstavljaju i akteri trećih strana, poput podizvođača, koji mogu namjerno ili nenamjerno iskoristiti dodijeljena prava pristupa, dohvatiti osjetljive podatke, izmijeniti konfiguraciju dijela mreže itd.

Za izgradnju kibernetički sigurnog 5G sustava kojem svi možemo vjerovati, potrebne su usklađene odgovornosti, jedinstveni standardi i jasna regulacija [20]. Vrijeme će pokazati kako će širenje 5G mreže u Hrvatskoj, EU-u i ostatku svijeta utjecati na kvalitetu i živote ljudi, koliko su naši podaci sigurni i da li ćemo biti svjedoci kibernetičkih kriza uzrokovanih incidentima i napadima u kibernetičkom prostoru.

9. Literatura

[1] Panettieri, J. (25.8.2021.), ChannelE2E and After Nines Inc., „Huawei: Banned and Permitted In Which Countries? List and FAQ“, dostupno na: https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries [pristup 2.9.2021.]

[2] youtube.com, „Huawei's Founder Speaks To BBC“, 17:36-18:10 minuta, dostupno na: https://www.youtube.com/watch?v=vxoeLLq14zI [pristup 27.9.2021.]

[3] NIS Coopeation Group (siječanj, 2020.), CG Publication, „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures“, dostupno na: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468 [pristup 14.8.2021.]

[4] politico.eu (14.10.2020.), „Letter to EU telecom and trade ministers and to European Commissioners Thierry Breton, Margrethe Vestager and Valdis Dombrovskis“, dostupno na: https://www.politico.eu/wp-content/uploads/2020/10/Clean-MEPs-letter-on-5G-and-trade-141020-1.pdf [pristup 2.9.2021.]

[5] HUAWEI TECHNOLOGIES CO., LTD. (prosinac, 2019.), „Towards a Trustworthy Foundation to Enhance the Security of EU 5G Networks“, dostupno na: https://huawei.eu/file-download/download/public/2504 [pristup 20.3.2021.]

[6] Lourenço, M., Marinos, L. (studeni, 2019.), „ENISA THREAT LANDSCAPE FOR 5G NETWORKS“, dostupno na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/view/++widget++form.widgets.fullReport/@@download/ENISA+threat+landscape+for+5G+Networks.pdf [pristup 1.9.2021.]

[7] HAKOM, „Zašto 5G“, dostupno na: https://www.hakom.hr/hr/zasto-5g/384 [pristup 29.8.2021.]

[8] Ericsson, „A guide to 5G network security“, dostupno na: https://www.ericsson.com/en/security/a-guide-to-5g-network-security#:~:text=Horizontal%20security%20will%20also%20protect,always%20confidentiality%20and%20integrity%20protected.&text=Transport%20networks%20play%20an%20important,between%20all%205G%20network%20functions [pristup 3.4.2021.]

[9] sdx central (travanj, 2021.), „Network Function (NF)“, dostupno na: https://www.sdxcentral.com/resources/glossary/network-function [pristup 6.2.2022.]

[10] Telco Cloud Bridge, „C-RAN vs Cloud RAN vs vRAN vs O-RAN- A simple Guide!“, dostupno na: https://telcocloudbridge.com/blog/c-ran-vs-cloud-ran-vs-vran-vs-o-ran [pristup 31.8.2021.]

[11] Wikipedia, slobodna enciklopedija (prosinac, 2021.), „OSI model“, dostupno na: https://hr.wikipedia.org/wiki/OSI_model [pristup 6.2.2022.]

[12] Peterson, L., Sunay, O., 5G Mobile Networks: A Systems Approach, „5G Mobile Networks: A Systems Approach, Chapter 3:00 Basic Architecture“, dostupno na: https://5g.systemsapproach.org/arch.html [pristup 1.9.2021.]

[13] SDxCentral Studios (9.10.2014.), „What Is NFV MANO?“, dostupno na: https://www.sdxcentral.com/networking/nfv/mano-lso/definitions/nfv-mano [pristup 12.2.2022.]

[14] Yang, J., Johansson, T., Science China (prosinac, 2020.), „An overview of cryptographic primitives for possible use in 5G and beyond“, dostupno na: https://link.springer.com/content/pdf/10.1007/s11432-019-2907-4.pdf [pristup 3.7.2021.]

[15] Tittel, E. (ožujak, 2020.), cisco.com, „SDN vs. NFV: What's the difference?“, dostupno na: https://www.cisco.com/c/en/us/solutions/software-defined-networking/sdn-vs-nfv.html [pristup 6.2.2022.]

[16] Rommer, S., Hedman, P., Olsson, M., Frid, L., Sultana, S, Mulligan, C., (2019.), „5G CORE NETWORKS Powering Digitalization“, Academic Press, ISBN: 978-0-08-103009-7, dostupno na: https://vdoc.pub/documents/5g-core-networks-powering-digitalization-1m4gl60n7jgo [pristup 15.4.2022.]

[17] 3GPP 2021., 3GPP A Global Initiative, The Mobile Broadband Standard, dostupno na: https://www.3gpp.org [pristup 16.5.2021.]

[18] 3GPP A Global Initiative, dostupno na: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501 [pristup 25.9.2021.]

[19] Dialogic, „Universal Subscriber Identity Module (USIM)“, dostupno na: https://www.dialogic.com/glossary/universal-subscriber-identity-module-usim [pristup 12.2.2022.]

[20] Huawei (2019.), „Partnering with the Industry for 5G Security Assurance“, dostupno na: https://www-file.huawei.com/-/media/corporate/pdf/trust-center/huawei-5g-security-white-paper-4th.pdf?la=en [pristup 13.8.2021.]

[21] Molenaar, R. (lipanj, 2020.), NetworkLessons.com, „IPsec (Internet Protocol Security)“, dostupno na: https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security [pristup 15.2.2022.]

[22] Ribbon Communications Operating Company, Inc., „What is an IP Multimedia Subsystem (IMS)?“, dostupno na: https://ribboncommunications.com/company/get-help/glossary/ip-multimedia-subsystem-ims [pristup 29.5.2021.]

[23] ETSI (listopad, 2018.), „5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.2.2000 Release 15)“, dostupno na: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.02.00_60/ts_133501v150200p.pdf [pristup 12.2.2022.]

[24] GSMA (2021.), „Network Equipment Security Assurance Scheme (NESAS)“, dostupno na: https://www.gsma.com/security/network-equipment-security-assurance-scheme [pristup 4.7.2021.]

[25] GSMA (2021.), „NESAS Security Auditors“, dostupno na: https://www.gsma.com/security/nesas-security-auditors [pristup 16.9.2021.]

[26] GSMA (5.2.2021.), „FS.16 – NESAS Development and Lifecycle Security Requirements v.2.0“, dostupno na: https://www.gsma.com/security/resources/fs-16-network-equipment-security-assurance-scheme-dispute-resolution-process [pristup 4.7.2021.]

[27] 3GPP 2021., 3GPP A Global Initiative, The Mobile Broadband Standard, „SA3 – Security“, dostupno na: https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security [pristup 4.7.2021.]

[28] Xiaomi news (rujan, 2020.), „How to test 5G to be sure the code and hardware are safe?“, dostupno na: https://www.xiaomist.com/2020/09/how-to-test-5g-to-be-sure-code-and.html [pristup 5.6.2022.]

[29] GSMA (2021.), „NESAS Participating Vendors“, dostupno na: https://www.gsma.com/security/nesas-participating-vendors [pristup 5.8.2021.]

[30] Weissberger, A. (15.3.2022.), IEEE Communications Society, „Gartner's Magic Quadrant for 5G Network Infrastructure for Communications Service Providers“, dostupno na: https://techblog.comsoc.org/2022/03/15/gartners-magic-quadrant-for-5g-network-infrastructure-for-communications-service-providers [pristup 23.5.2022.]

[31] Gartner (veljača, 2022.), „Magic Quadrant for 5G Network Infrastructure for Communications Service Providers“, dostupno na: https://www.gartner.com/resources/746400/746462/Figure_1_Magic_Quadrant_for_5G_Network_Infrastructure_for_Communications_Service_Providers.png?reprintKey=1-299M6Q7A [pristup 23.5.2022.]

[32] ericsson.com (2021.), „Ericsson in Sweden“, dostupno na: https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/sweden [pristup 23.6.2021.]

[33] ericsson.com (17.9.2018.), „Ericsson automated smart factory operational in China“, dostupno na: https://www.ericsson.com/en/press-releases/2019/9/ericsson-automated-smart-factory-operational-in-china [pristup 7.8.2021.]

[34] Mello, G., (25.11.2019.), Reuters, „Ericsson to invest over $230 million in Brazil to build new 5G assembly line“, dostupno na: https://www.reuters.com/article/us-ericsson-brazil-idUSKBN1XZ2D5 [pristup 7.8.2021.]

[35] ericsson.com (15.3.2021.), „Ericsson USA 5G Smart Factory recognized as 'Global Lighthouse' by the World Economic Forum“, dostupno na: https://www.ericsson.com/en/press-releases/2021/3/ericsson-usa-5g-smart-factory-recognized-as-global-lighthouse-by-the-world-economic-forum [pristup 7.8.2021.]

[36] ericsson.com (2021.), „Switch on a better 5G network“, dostupno na: https://www.ericsson.com/en/5g/5g-networks [pristup 3.7.2021.]

[37] ericsson.com, Norrman, K., Kumar Nakarmi, P., Fogelström, E. (ožujak, 2021.), „5G security - enabling a trustworthy 5G system“, dostupno na: https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security---enabling-a-trustworthy-5g-system [pristup 5.8.2021.]

[38] Wikipedia, The Free Encyclopedia, „Nokia“, dostupno na: https://en.wikipedia.org/wiki/Nokia [pristup 7.8.2021.]

[39] Nokia (3.7.2019.), „Nokia's digitalization of its 5G Oulu factory recognized by the World Economic Forum as an Advanced 4th Industrial Revolution Lighthouse“, dostupno na: https://www.nokia.com/about-us/news/releases/2019/07/03/nokias-digitalization-of-its-5g-oulu-factory-recognized-by-the-world-economic-forum-as-an-advanced-4th-industrial-revolution-lighthouse [pristup 8.8.2021.]

[40] Nokia (25.10.2018.), „Nokia Chennai factory first to manufacture 5G radio equipment in India“, dostupno na: https://www.nokia.com/about-us/news/releases/2018/10/25/nokia-chennai-factory-first-to-manufacture-5g-radio-equipment-in-india [pristup 8.8.2021.]

[41] Nokia, „Think beyond radio. 5G requires so much more“, dostupno na: https://www.nokia.com/networks/5g/mobile/explore-5g-solutions [pristup 8.8.2021.]

[42] Nokia, „Cyber security“, dostupno na: https://www.nokia.com/networks/portfolio/cyber-security [pristup 9.8.2021.]

[43] Nokia, „NetGuard XDR Security Operations“, dostupno na: https://www.nokia.com/networks/solutions/netguard-xdr-security-operations/#features-and-benefits [pristup 9.8.2021.]

[44] Nokia, „Privacy challenges and security solutions for 5G networks“, dostupno na: https://www.nokia.com/networks/insights/privacy-challenges-security-solutions-5g-networks [pristup 9.8.2021.]

[45] Wikipedia, The Free Encyclopedia, „Huawei“, dostupno na: https://hr.wikipedia.org/wiki/Huawei [pristup 9.8.2021.]

[46] Huawei (4.3.2021.), „Huawei and China Mobile Guangdong Piloted 5G Indoor Distributed Massive MIMO“, dostupno na: https://www.huawei.com/en/news/2021/3/chinamobile-guangdong-5g-distributed-m-mimo [pristup 10.8.2021.]

[47] Huawei (26.1.2021.), „HUAWEI LAUNCHES FIRST-OF-ITS-KIND EUROPEAN PRODUCTION PLANT“, dostupno na: https://huawei.eu/press-release/huawei-launches-first-its-kind-european-production-plant [pristup 10.8.2021.]

[48] Huawei, 5G, dostupno na: https://carrier.huawei.com/en/spotlight/5g [pristup 11.8.2021.]

[49] Batas, S., Men, M., Smitham, M. (prosinac, 2019.), „Towards a Trustworthy Foundation to Enhance the Security of EU 5G Networks“, dostupno na: https://huawei.eu/file-download/download/public/2504 [pristup 11.8.2021.]

[50] Huawei, „Does Huawei have ties to the Communist Party of China (CPC)?“, dostupno na: https://www.huawei.com/en/facts/question-answer/does-huawei-have-ties-to-the-cpc [pristup 11.8.2021.]

[51] J. Williamson, P., Wu. X., Yin. E. (lipanj, 2019.), Ivey Business Journal, „Learning from Huawei’s Superfluidity“, dostupno na: https://iveybusinessjournal.com/learning-from-huaweis-superfluidity [pristup 11.8.2021.]

[52] Huawei (5.3.2019.), „Huawei Cyber Security Transparency Centre Opens in Brussels“. dostupno na: https://www.huawei.com/en/news/2019/3/huawei-cyber-security-transparency-centre-brussels [pristup 14.8.2021.]

[53] Huawei (9.6.2021.), „Huawei Opens Its Largest Global Cyber Security and Privacy Protection Transparency Center in China“, dostupno na: https://www.huawei.com/en/news/2021/6/huawei-largest-global-cyber-security-privacy-protection-transparency-center [pristup 14.8.2021.]

[54] IEEE Spectrum (srpanj, 2007.), „The Athens Affair“, dostupno na: https://www.spinellis.gr/pubs/jrnl/2007-Spectrum-AA/html/PS07.pdf [pristup 22.6.2021.]

[55] Prevelakis, V., Spinellis, D. (29.6.2007.), IEEE Spectrum, „The Athens Affair“, dostupno na: https://spectrum.ieee.org/telecom/security/the-athens-affair [pristup 22.6.2021.]

[56] Obiko Pearson, N. (1.7.2020.), Bloomberg, „Did a Chinese Hack Kill Canada’s Greatest Tech Company?“, dostupno na: https://www.bloomberg.com/news/features/2020-07-01/did-china-steal-canada-s-edge-in-5g-from-nortel [pristup 7.5.2022.]

[57] Lepido, D. (30.4.2019.), Bloomberg, „Vodafone Found Hidden Backdoors in Huawei Equipment“, dostupno na: https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment [pristup 22.6.2021.]

[58] Robertson, J. Tarabay Bloomberg, J. (17.12.2021.), Bloomberg, „Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack“, dostupno na: https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack [pristup 7.5.2022.]

[59] Pongratz, S. (14.3.2022.), Dell'Oro, „Key Takeaways – 2021 Total Telecom Equipment Market“, dostupno na: https://www.delloro.com/key-takeaways-2021-total-telecom-equipment-market [pristup 24.4.2022.]

[60] Bartholomew, C. (2020.), Winter 2020 Issues in Science and Technology, Arizona State University, „China and 5G“, dostupno na: https://issues.org/china-and-5g [pristup 24.4.2022.]

[61] CIS (19.12.2011.), „Advanced Persistent Threat napadi“, dostupno na: https://www.cis.hr/dokumenti/2988-advanced-persistent-threat-napadi.html [pristup 19.5.2022.]

[62] Creemers, R., Webster, G. (20.8.2021.), Stanford University, „Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1 2021)“, dostupno na: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021 [pristup 28.8.2021.]

[63] Wagner, J. (1.6.2017.), The Diplomat, „China’s Cybersecurity Law: What You Need to Know“, dostupno na: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know [pristup 4.8.2021.]

[64] OneTrust DataGuidance, „CYBERSECURITY LAW OF THE PEOPLE’S REPUBLIC OF CHINA“, dostupno na: https://www.dataguidance.com/sites/default/files/en_cybersecurity_law_of_the_peoples_republic_of_china_1.pdf [pristup 4.8.2021.]

[65] Wikipedia, slobodna enciklopedija (kolovoz, 2021.), „Company Law of the People's Republic of China“, dostupno na: https://en.wikipedia.org/wiki/Company_Law_of_the_People%27s_Republic_of_China [pristup 11.8.2021.]

[66] Bureau du Conseiller Economique et Commercial à Madagascar (17.10.2019.), „Company Law of the People's Republic of China“, dostupno na: http://mg.mofcom.gov.cn/article/policy/201910/20191002905610.shtml [pristup 27.9.2021.]

[67] Wikipedia, slobodna enciklopedija (kolovoz, 2021.), „National Intelligence Law of the People's Republic of China“, dostupno na: https://en.wikipedia.org/wiki/National_Intelligence_Law_of_the_People%27s_Republic_of_China [pristup 11.8.2021.]

[68] China Law Translate (3.11.2011.), „Counter-espionage Law“, dostupno na: https://www.chinalawtranslate.com/en/anti-espionage [pristup 12.8.2021.]

[69] European Court of Human Rights Council of Europe (listopad, 2013.), „European Convention on Human Rights“, dostupno na: https://www.echr.coe.int/documents/convention_eng.pdf [pristup 24.4.2022.]

[70] Heiderich, M. (studeni, 2019.), Cure53, „Analysis-Report “Study the Great Nation” 08.-09.2019“, dostupno na: https://cure53.de/analysis_report_sgn.pdf [pristup 24.4.2022.]

[71] Finite State (26.6.2019.), „Finite State Supply Chain Assessment Huawei Technologies Co., Ltd.“, dostupno na: https://info.finitestate.io/hubfs/Collateral/Finite%20State%20Supply%20Chain%20Assessment-%20Huawei%20Technologies.pdf [pristup 24.4.2022.]

[72] CVE security vulnerability database. Security vulnerabilities, exploits, references and more, dostupno na: https://www.cvedetails.com [pristup 24.4.2022.]

[73] NIS Coopeation Group (9.11.2019.), „EU coordinated risk assessment of the cybersecurity of 5G networks“, dostupno na: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132 [pristup 17.8.2021.]

[74] Total Croatia News (1.2.2020.), „Croatia to Define Criteria for 5G Equipment Suppliers by Year's End“, dostupno na: https://www.total-croatia-news.com/business/41219-5g [pristup 20.8.2021.]

[75] Czech Republic Government (3.5.2019.), „The Prague Proposals. The Chairman Statement on cyber security of communication networks in a globally digitalized world. Prague 5G Security Conference“, dostupno na: https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf [pristup 14.8.2021.]

Životopis

Katarina Matić rođena je 1981. u Zadru, gdje je završila osnovnu školu i gimnaziju. Visokoškolsko obrazovanje stekla je na Fakultetu elektrotehnike i računarstva Sveučilišta u Zagrebu, gdje je diplomirala 2004. na smjeru Telekomunikacije i informatika.

Od 2004. do 2019. zaposlena je na Hrvatskoj radioteleviziji (HRT) u odjelu Informatika gdje vodi projekte modernizacije, administracije, održavanja računalnih mreža i IT sustava na platformama Linux i Windows. Sudjeluje u projektu IP prijenosa audio i video signala s udaljenih lokacija i optimizacije kvalitete prijenosa podataka uživo, digitalizaciji video sustava HRT-a, umrežavanju i opremanju centara HRT-a te drugim multimedijalnim projektima (Olimpijske igre, Svjetsko nogometno prvenstvo, Bingo, Loto 7, Parlamentarni izbori, Prix Marulić, Circom itd.).

Od 2019. zaposlena je u Hrvatskoj regulatornoj agenciji za mrežne djelatnosti (HAKOM) kao viši IT inženjer u odjelu IS/IT. Vodi i sudjeluje u planiranju, izgradnji i razvoju moderne ICT infrastrukture, informacijskih servisa i sustava. Uključena je u projekte vezane za informacijsku sigurnost na razini HAKOM-a kao i nacionalnoj i međunarodnoj razini.

Tijekom višegodišnjeg radnog iskustva stekla je široka stručna znanja iz područja ICT infrastrukture, mrežnih tehnologija i informacijske sigurnosti. Certificirana je Linux inženjerka te Cisco mrežna inženjerka profesionalne razine.

Biography

Katarina Matić was born in 1981 in Zadar. In 2004 she acquired M.Eng. title from the Faculty of Electrical Engineering and Computing, University of Zagreb.

From 2004 to 2019 she worked at Croatian Radiotelevision (HRT) in the IT department, where she managed modernization, administration and maintenance of IP networks and IT systems on Linux and Windows platforms. She participated in the project of IP transmission of audio and video streams from remote locations and optimization of the quality of live data transmission, digitization of HRT's video system, HRT IP networking and equipping and other multimedia projects (Olympic Games, World Football Championship, Bingo, Loto 7, Parliamentary elections, Prix Marulić, Circom, etc.).

Since 2019, she has been employed as a senior IT engineer at the Croatian Regulatory Authority for Network Industries (HAKOM) in the IS/IT department. She leads and participates in the planning, construction and development of modern ICT infrastructure, information services and systems. She is involved in both national and international projects related to information security.

During many years of work experience, she acquired extensive professional knowledge in the ICT infrastructure field, network technologies and information security. She is a certified Linux engineer and a professional Cisco network engineer.