FiCom ry

ICT-alan suomalainen edunvalvoja, jonka tavoitteena on edistää jäsentensä liiketoiminta-mahdollisuuksia ja parantaa alan kilpailukykyä.

FiComin jäsenet ovat yhteiskunnan digitaalisen ja teknologisen kehityksen mahdollistajia.

Markkinaehtoisuus, teknologia-neutraalius ja ratkaisukeskeisyys!

Toimintaamme ohjaavat asiantuntemus, aktiivisuus ja avoimuus.

Jäsenet:

Cinia, Cisco, Digita, DNA, elisa, Ericsson, Erillisverkot, Ficolo, Finnet-liitto, Geomatikk, Google, hp, maxisat, Microsoft, nestor cables, Rejlers, Telia

Kannattajajäsen:

Meta

Viestintäverkkojen tietoturvallisuuden sääntely

- **SVPL (sähköisen viestinnän palvelulaki)**
  - **29 luku Viestintäverkkojen ja viestintäpalvelujen laatuvaatimukset, jossa mm.**
    - **243 §** Tietoturvavaatimukset verkkojen ja palvelujen koko elinkaaren ajalle
    - **244 §** sisältää em. §:ää koskevan 16 kohtaisen määräyksenantovaltuuden
    - **244 a §** Viestintäverkon kriittisissä osissa käytettävät laitteet
    - **244 b §** Verkkoturvallisuuden neuvottelukunta
  - **33 luku Tietoturvan ja häiriöiden hallinta sekä häiriöistä ilmoittaminen, jossa mm.**
    - **272 §** Toimenpiteet tietoturvan toteuttamiseksi
    - **273 §** Velvollisuus korjata häiriö
  - **35 luku Varautuminen, jossa mm.**
    - **281 §** Velvollisuus varautua normaaliolojen häiriötilanteisiin ja poikkeusoloihin
    - **282 §** Varautumissuunnittelu

- **Traficomin määräyksiä**
  - Määräys teletoiminnan tietoturvasta (**määräys 67**)
  - Tietoturvan toteuttamista koskevat vähimmäisvaatimukset. Määräyksellä pyritään varmistamaan, että tietoturvatekijät huomioidaan rutiininomaisesti osana verkkojen toteutusta.
  - Määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista (**määräys 54**)
  - Minimivelvoitteet laitteiden tehonsyötön varmistukselle, laitteiden ja yhteyksien varmistamiselle sekä laitteiden fyysiselle suojaamiselle
  - Määräys teletoiminnan häiriötilanteista (**määräys 66**)
  - Velvoitteet teleyrityksille tietoturva- ja toimivuushäiriöiden havaitsemista ja hallintaa kuin niistä ilmoittamista ja tilastointia varten
  - Suositus teletoiminnan varautumisesta (**suositus 311**) lakiin perustuvien varautumisvelvoitteiden täyttämisestä
  - Määräys viestintäverkkojen ja -palvelujen laadusta ja yleispalvelusta (**määräys 58**)
  - Viestintäverkkojen ja -palvelujen toimintavarmuuden, suorituskyvyn, luotettavuuden ja laadun mittaaminen ja varmistaminen
  - Määräys hätäliikenteen teknisestä toteutuksesta ja varmistamisesta (**määräys 33**)
  - Varmistetaan hätäpuhelujen normaaleja puheluja paremmat onnistumismahdollisuudet erilaisissa viestintäverkon ruuhka- ja häiriötilanteissa sekä hätäpuheluiden ja hätätekstiviestien sekä niihin liittyvän hätäpalvelun kannalta olennaisen informaation siirtyminen viestintäverkoista hätäkeskuksiin.
  - Määräys viestintäverkon kriittisistä osista

FiCom

Liikenne- ja viestintävaliokunta 11.2.2022
Operaattoreiden varautuminen

Yleistä operaattoreiden varautumisesta – tietoturvan hallinta

Vesa Vuoti, DNA

Jaakko Wallenius, Elisa

Open RAN – mitä se on ja mitä se tarjoaa?

Timo Hietalahti, Telia

Yleistä operaattoreiden varautumisesta

Vesa Vuoti

DNA Oyj

Operaattorin prosessit tietoturvan hallintaan

Operaattorit suunnittelevat ja toteuttavat jatkuvasti proaktiivisesti tietoturvan hallintaan liittyviä prosesseja ja asiakasvaatimukset ovat tässä keskeisenä ajurina:

1. Toimintaympäristöön liittyvät riskit ja uhat evaluoidaan ja tunnistetaan mm. standardoinnista, viranomaislähteistä ja omasta tuotannosta.
2. Verkon suojausvaatimukset ja -standardit ovat tärkeä tekijä jo toimittaja-valinnoissa ja suojausmekanismit kehitetään sekä sisäisesti, että yhdessä valittujen laite- ja ohjelmistotoimittajien kanssa.

   Kriittiset järjestelmät suunnitellaan siten, että ne voivat toimia autonomisesti internetistä riippumatta ja niiden toiminta on georedundanttisesti varmistettu.

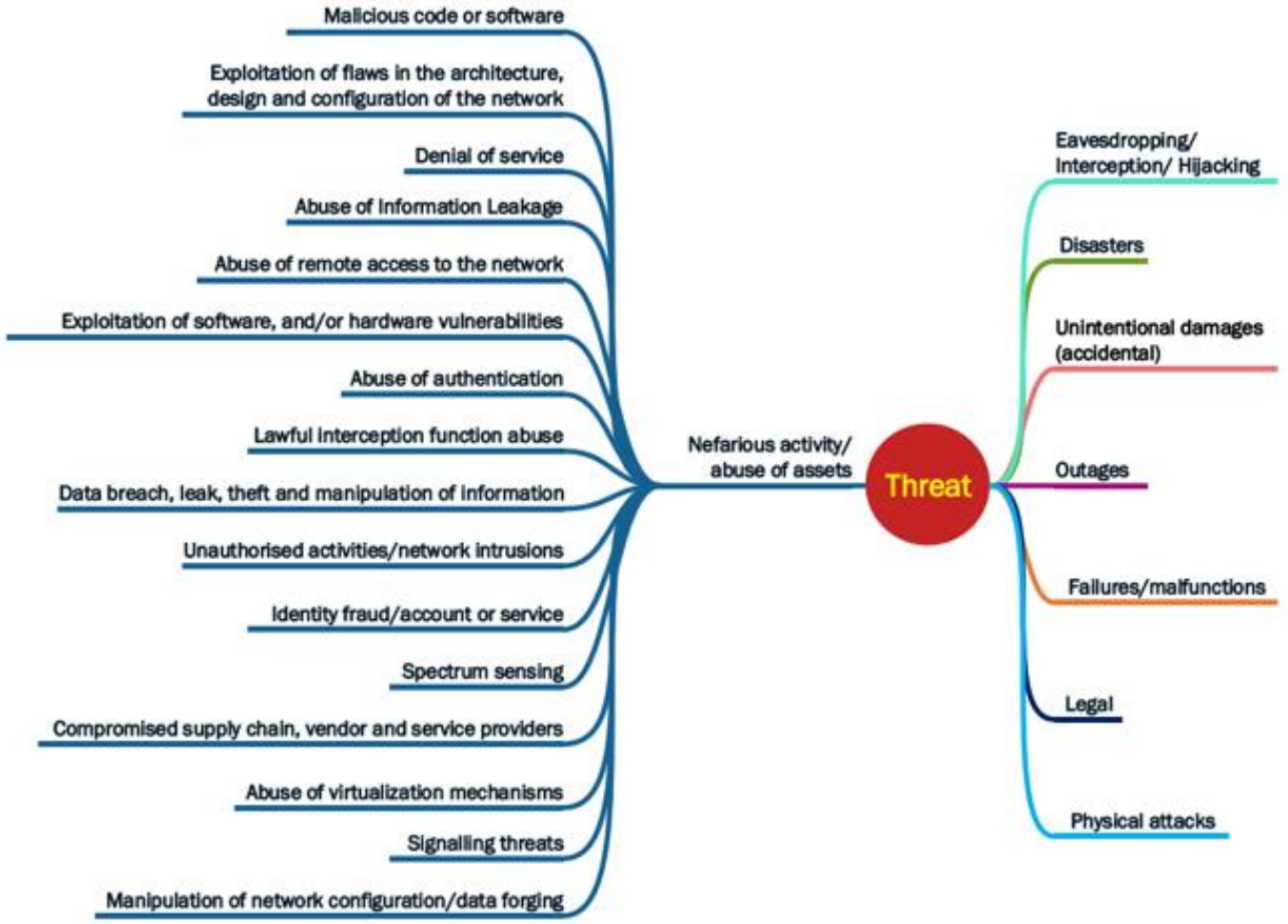
   Monitoimittajaympäristön operaattorivetoinen suunnittelu ja ylläpito pienentävät toimittajakohtaisia riskikasaumia.

   Verkon suunnittelussa suojataan tarvittavat hallintayhteydet ja vain välttämättömät rajapinnat ovat suoraan kytköksissä internetiin.
3. Haavoittuvuuksien ja hyökkäyksien tunnistaminen ja torjunta perustuu laajaan kykyyn toimia 24/7 (SOC, Security Operations Center) ja henkilöstön ja yhteistyökumppaneiden vahvaan osaamiseen.
4. Tunnistetut ongelmat käynnistävät välittömät ongelma-analyysit häiriönhallintaprosessin mukaisesti. Prosessi päivittyy tarpeen mukaan.
5. Varautumissuunnitelman mukaisia palautumismekanismeja päivitetään ja testataan säännöllisesti.



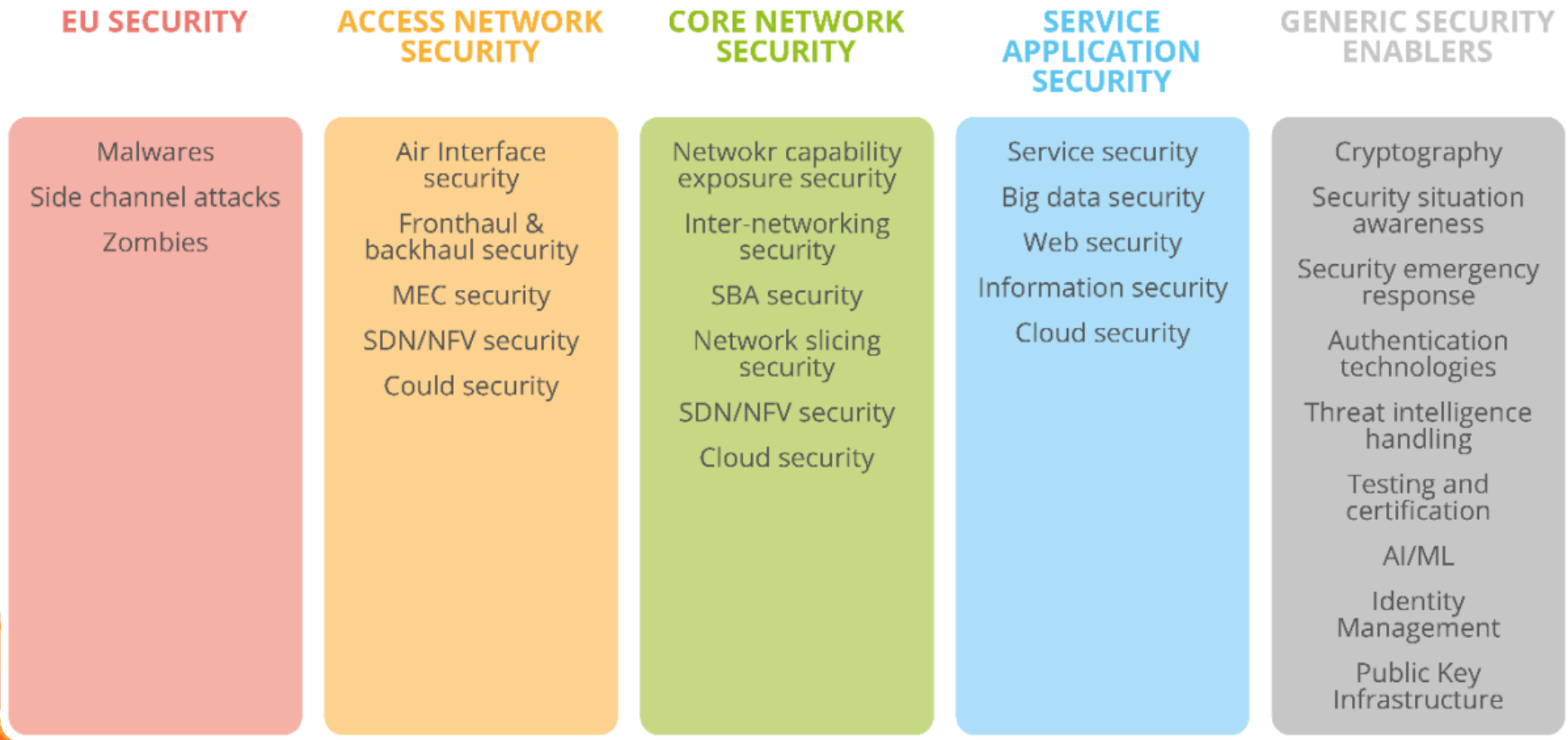
Lähde: The NIST Cybersecurity Framework

5G-verkkojen uhkamaisema



https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/at_download/fullReport

5G-verkkojen turvallisuusdomainit



https://www.enisa.europa.eu/publications/security-in-5g-specifications/at_download/fullReport

5G-verkkoihin liittyviä turvallisuusnäkökulmia

- Eurooppavetoinen ENISA-ETSI-3GPP on polku tunnistetuista ja uusista tietoturvauhkista teknologiastandardiin.
- 5G-standardissa on huomioitu sekä edellisten sukupolvien heikkoudet että uuden teknologian turvavaatimukset paremmin kuin koskaan aikaisemmin.
- Standardoinnissa ja käyttöönotossa on myös huomioitava, että 5G-verkkojen hyödyntämisen edetessä otetaan käyttöön merkittävä määrä uusia käyttötapauksia ja 5G-verkkoihin kytkettyjen laitteiden määrä kasvaa jatkuvasti.
- Rikolliset ryhmittymät, yksittäiset hakkerit ja valtiot kehittävät jatkuvasti uusia keinoja tietomurtojen mahdollistamiseksi.
- Tietoturvauhkien globaali ja paikallinen tiedonvaihto yhdessä operaattorien varautumismekanismien kanssa parantaa ennaltaehkäisyä kaikilla tiedonsiirron osa-alueilla.
- Em. näkökulmien huomioiminen jo verkkoteknologian hankinta- ja suunnitteluvaiheessa tulee jatkossa korostumaan entisestään kaikilla operaattoreilla.

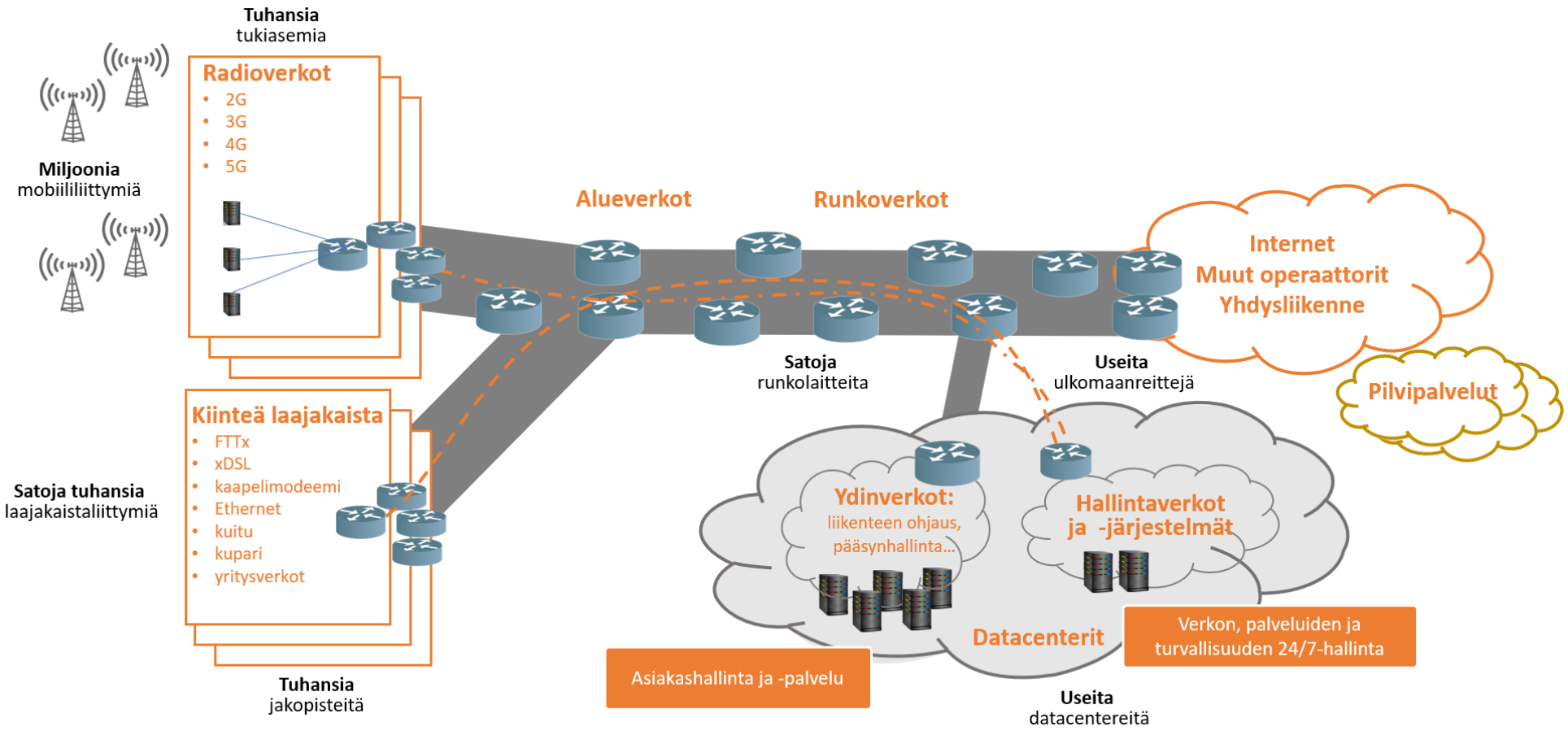
Tietoturvan hallinta

Jaakko Wallenius

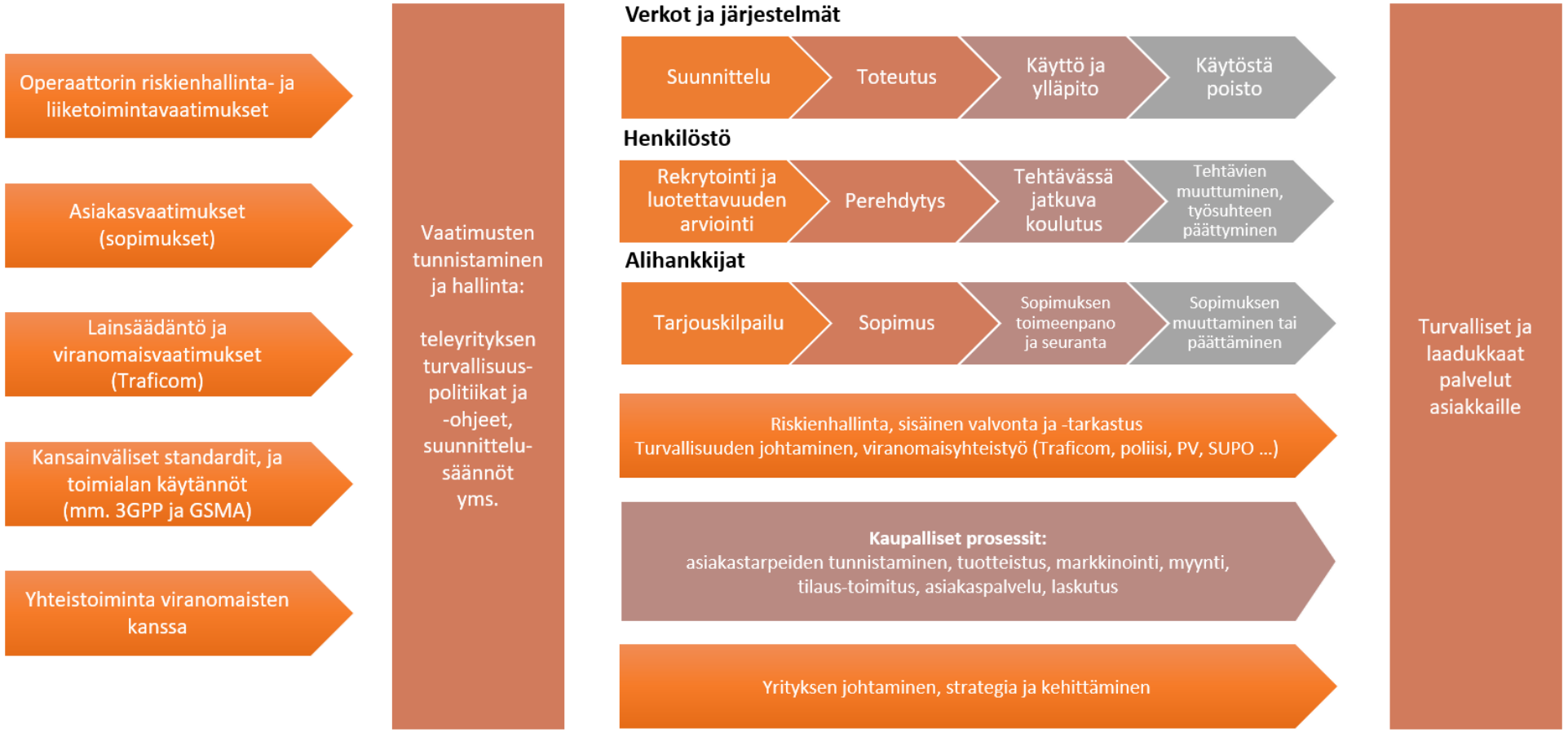
Elisa Oyj

Teleyritysten verkot koostuvat laajoista ja ositetuista kokonaisuuksista - tavoitteena laatu, varmuus ja turvallisuus

Muutosten suunnittelu, hallinta ja suunnitelmallinen toteuttaminen ovat kriittisiä verkon toimivuuden ja palveluiden laadun varmistamiseksi



Teleyrityksen turvallisuuden hallinta perustuu toimintaprosesseissa tehtäviin asioihin



Operaattorin riskienhallinta- ja liiketoimintavaatimukset

Asiakasvaatimukset (sopimukset)

Lainsäädäntö ja viranomaisvaatimukset (Traficom)

Kansainväliset standardit, ja toimialan käytännöt (mm. 3GPP ja GSMA)

Yhteistoiminta viranomaisten kanssa



Open RAN
– mitä se on ja mitä se tarjoaa?

Timo Hietalahti

Telia Finland Oyj

Open Radio Access Network (O-RAN)



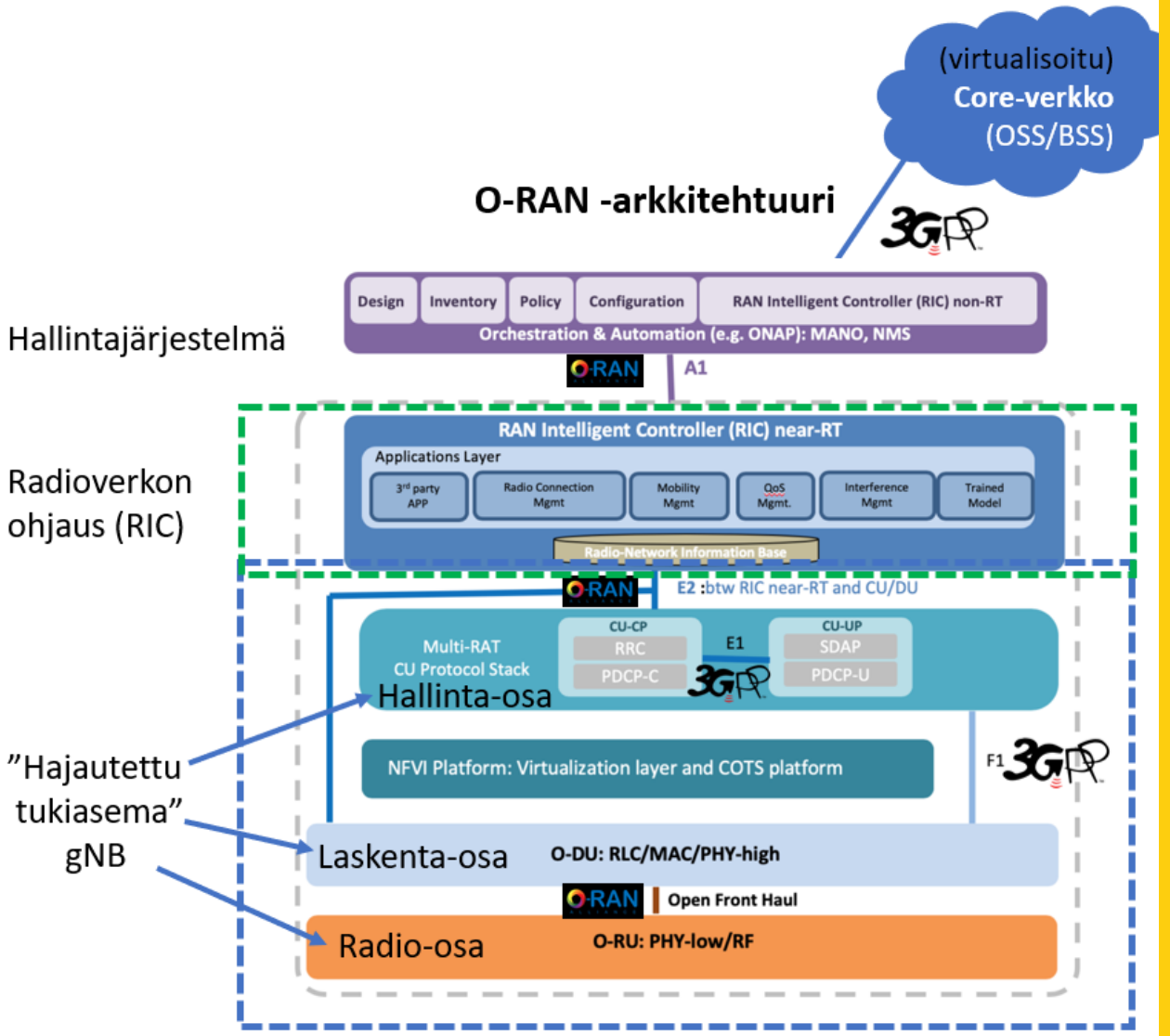
- Open RAN on kehitetty operaattoreiden lähtökohdista
  - julkaistiin v. 2018
  - O-RAN Alliance, https://www.o-ran.org/
  - 10 operaattorivetoista työryhmää yhteistyössä laitevalmistajien kanssa
  - noin 30 operaattoria → 240 osallistujaorganisaatiota
- TCO:n alentaminen
  - kilpailun lisääminen ja ”perinteisten” toimittajasidonnaisuuksien purkaminen
- RAN:in avoimuus
  - avoimet standardoidut rajapinnat ja infrastruktuuri mahdollistavat eri laitetoimittajien yhteentoimivuuden
- Ohjelmoitavuus
  - HW/SW erottaminen, sama kehityssuunta jo ns. Cloud RAN -evoluutiossa perinteisillä laitevalmistajilla
  - palvelujen optimointi ja toiminnan tehostaminen tekoälyn ja koneoppimisen avulla
  - jokainen verkon komponentti saatetaan keskustelemaan ohjelmistojen välityksellä, tarvittaessa reaaliaikaisesti
- Nopeampi palveluiden ja sovellusten kehittäminen ja julkaisu markkinoille
  - 5G on keskeinen ajuri yhdessä virtualisoinnin/pilviarkkitehtuurin kehittymisen kanssa

O-RAN Alliance, Board Members 2020-22

Company	Type
AT&T	Founding Member
China Mobile	Founding Member
Deutsche Telekom	Founding Member
NTT DOCOMO	Founding Member
Orange	Founding Member
Bharti Airtel	Elected Member
DISH Network	Elected Member
KDDI	Elected Member
Rakuten Mobile	Elected Member
Reliance Jio	Elected Member
Singtel	Elected Member
TIM	Elected Member
Telefonica	Elected Member
Verizon	Elected Member
Vodafone	Elected Member

Mikä O-RAN?

- Arkkitehtuurin osat voidaan valita ja rakentaa itsenäisesti
- Standardoinnissa 3GPP:llä merkittävä rooli ”tukiasemaosassa”
- CU-DU, CU-CP ja CU-UP rajapinnat haasteellisia
- Tavoitteena “ohjelmoitava” ja itseoppiva radioverkko
- 4G- ja 5G RAN -yhteensopivuus
- Virtualisoidut verkkoelementit
- Avoimet ohjelmistorajapinnat ja API:t
- Älykäs ohjaus (RIC)
- HUOM! RIC optionaalinen



* https://telecominfraproject.com/how-we-work/

O-RAN: haasteet operaattoreille

- Radioverkon uudelleenjärjestelyt
  - eri verkkoelementtien yhteensovittaminen ja toimivuuksien testaaminen vaatii merkittävästi aikaa ja resursseja (HUOM: TIP*)
  - suorituskyvyn varmistaminen ja sen kehittyminen
  - ominaisuuksien ja roadmappien yhteensovittaminen, elinkaarihallinta, eri laitevalmistajien yhteensopivuus
  - jokainen mobiiliverkkototeutus käytännössä uniikki
- Rinnakkaiselo nykyisten verkkojen kanssa
  - 2G, 3G, 4G ja myös 5G
  - useiden tuhansien tukiasemien saumaton siirtymä varmistettava
  - vie aikaa useita vuosia, vanhempien teknologioiden poistumat sovitettava
  - myös uusien palveluiden ja ominaisuuksien saaminen verkkoihin voi todellisuudessa viivästyä
- Välttämätön kuitusaatavuus varmistettava
  - kustannustehokkaat yhteydet eri verkkoelementtien välille päästä päähän (Core - RIC- CU- DU ja RU)
  - Tarvitaan, jotta saavutetaan arkkitehtuurin mahdollistamat hyödyt ja tehokkuudet reaaliaikaisuusvaatimus huomioiden
- Verkon hallinta ja ylläpito
  - ei selkeää vastuullista toimijaa, joka kehittäisi koko RAN-suorituskykyä → jää käytännössä vain operaattorin vastuulle
  - kustannukset voivat ”karata” esim. hallintajärjestelmistä ja elinkaaren hallinnan kompleksisuuksista johtuen

Tulevaisuus

- Mitä on jo maailmalla käytössä?
  - Rakuten, Vodafone, Telefonica (Peru) ym.
- Tietoturva ja vaikutukset kriittisten verkkoelementtien määrittelyyn
  - RIC keskeinen verkon elementti, johon liittyy useita palveluita, toiminnallisuuksia ja ohjausominaisuuksia
  - hallintajärjestelmiä ja niiden ominaisuuksia hajautetaan → saattaa vaikeuttaa kriittisyysmäärittelyä
  - pääsy järjestelmän useisiin eri osiin maan rajojen ulkopuolelta tulee todennäköisesti välttämättömäksi
- Aikatauluarvioita
  - ajankohtaiset testaukset todennäköisesti vuosikymmenen puolivälistä alkaen
  - eri osia O-RAN -konseptista testataan ensin, 6G-teknologia ehkä ensimmäinen laajempi kokonaisuus

