

1) Väga hästi haakuvad kohad (tõsta esile kui “joondunud”)

1.1 Ühtne COP + mitme asutuse koostöö

Nortal röhutab sama põhivajadust: killustatud sensorivõimekus tekitab pimelaike ja vaja on ühist seirepilti ning koostööd teiste riiklike süsteemidega.

NORTAL

NORTAL

See on 100% sama, mida me röhutasime: “üks pilt, palju kasutajaid”.

1.2 Etapiline teostus (eelanalüüs → prototüüp → MVP → laiendused)

PPA enda etapistus on sama loogikaga nagu meie “prototype reality” (ingest → normaliseeri → track/event → kaart → alert).

Eelanalüüs

Nortal positsioneerib eelanalüüsi kui sisendi detailanalüüsile/prototüübile.

NORTAL

1.3 Rollid / õigused + auditeeritavus

Nortal ütleb selgelt, et tuleb kaardistada rollid, ligipääsusatasemed, RBAC/ABAC kaalutlused ja sensoripõhine nähtavus.

NORTAL

NORTAL

See haakub meie “multi-agency, masking/obfuscation, audit log” teljega.

1.4 Avatud standardite orientatsioon (SAPIENT, ASTERIX, MOSA, NATO STANAG)

Nortal toob standardid lauale samas vaimus: SAPIENT, ASTERIX, MOSA, U-space/UTM, NATO STANAG-id.

NORTAL

PPA turu-uuringus on sama minimaalne “SAPIENT, ASTERIX, MOSA” ootus.

Eelanalüüs

1.5 “Ei tohi olla SPOF” ja modulaarne alamsüsteemide lähenemine

Nortali arhitektuuripõhimõtted (“alamsüsteemid vahetatavad”, “SPOF ei tohi olla”) on sama MOSA mentaliteet, millele me panime rõhku.

NORTAL

2) Kohad, kus Nortali plaan läheb meie varasema jutuga pingesse (või vajab täpsustust)

Need ei ole “valed” ideed – pigem kohad, kus valesti sõnastatud nõue võib hiljem **hankes turgu ära tappa**, tekitada **integreerimisvõlg** või teha **reaalaja / suure mahu** vood valusaks.

2.1 “X-tee laadne” sensorvõrk vs reaalaja vood (radar/video/multicast)

Nortal eelistab “x-tee laadset lahendust, kus EDGE seadmed käituvad kui x-tee turvaserverid ja suudavad andmeid saata ka juhul kui keskserver ei ole kättesaadav”.

NORTAL

Meie varasem jutt oli sensorivoodes pigem: UDP/SSM multicast (video/radar), event/track bus, standardprotokollid, ja adapterid.

Miks see võib olla konflikt:

- X-tee paradigma on ajalooliselt *päring/vastus* ja dokumentide vahetus; see võib olla kohmakas *kõrgsagedusliku streaming* jaoks (radar video, FMV, tihe track feed).
- Kui “x-tee” tõlgendada kui “kõik sõnumid allkirjastatud ja keskne turvakiht”, võib see tekitada latentsust ja läbi-lõike pudelikaelu.

Mida eelanalüüsis töstatada:

- Kas “x-tee” on siin *metafoor* (turvaline, hajus, identiteedipõhine) või *reaalne tehnoloogiline valik*?
- Kui see on metafoor: sõnastada nõue ümber “zero-trust + identiteet + usaldusraamistik” ilma X-tee tehnoloogilise lukustuseta.

2.2 “EDGE krüpteerib ja allkirjastab kogu võrgu liikluse” – liiga absoluutne nõue

Nortal ütleb, et EDGE peab “krüpteerima ja allkirjastama kogu võrgu liikluse”.

NORTAL

Meie varasem arhitektuur eristas kihid: L2 (nt MACsec) / L4 (TLS/DTLS) / app-taseme allkirjad ainult seal, kus vaja (audit, nonrepudiation, RID trust).

Miks see on risk:

- “Kogu liiklus” allkirjastamine (eriti video/radar stream) võib olla CPU/latentsuse mõttes ebarealistlik või kallis.
- “Krüpteerimine” võib juba tulla link-layer (MACsec) või tunnelite kaudu; kui nõue pannakse EDGE-le absoluutseks, võib see turgu kitsendada.

Mida eelanalüüsis tõstatada:

- Täpsustada: **milline liiklus** peab olema allkirjastatud (nt juhtimis-/käsklus-, audit-kriitiline, RID trust) ja milline “ainult krüpteeritud transportiga”.
- Määrata kihipõhiselt: link-layer krüpto (site LAN), WAN tunnel/DTLS, ja vajadusel objektipõhine signatuur.

2.3 EDGE peab “tuvastama signaalist õhusõiduki ja selle tüübi”

Nortal kirjeldab EDGE-d kui komponenti, mis suudab tuvastada “sensori signaalist õhusõidukit ja selle tüüpi”.

NORTAL

Meie varasem lähenemine pigem: adapter/normaliseerija teeb protokolli-silla ja COP/fusion teeb koondloogika; sensori “AI” võib olla vendoris või eraldi.

Miks see võib olla vastuolus:

- Kui nõue lukustab “klassifikatsioon peab olema edge’is”, tekib uus turupiirang (mitte kõik sensorid/adapterid ei tee klassifikatsiooni ühtemoodi).
- Te riskite sellega, et “vendor edge” muutub de-facto mustaks kastiks.

Mida eelanalüüsis tõstatada:

- Klassifikatsioon = **valikuline** võime. Kohustuslikud on: *standardiseeritud output* (track/detection + metadata + timestamp + confidence fields).
- Sõnastada “EDGE võib teha klassifikatsiooni, aga COP peab suutma töötada ka ilma selleta”.

2.4 Hajus “regionaalne + keskne COP” on hea – aga vajab andmemudeli / replikatsiooni otsust

Nortal tahab, et COP töötaks regionaalselt ka siis, kui keskne tase ei tööta, ja vastupidi.

NORTAL

See haakub “no SPOF” ideega, **aga** eelanalüüs peab vältima olukorda, kus hajus arhitektuur jäääb “sõnaliseks”.

Mida eelanalüüsis tõstatada (konkreetsete otsustuskohtadena):

- Kas regionaalne COP on “täisfunktionaalne” või “degradeeritud” (ainult kohalik nähtavus + store-and-forward)?
- Kuidas toimub **sündmuste/trackide replikatsioon** (event sourcing, message broker federation, “fused tracks only” vs “raw tracks also”)?
- Kuidas lahendada “kes on tõde” konfliktid (track ID-d, merge/split, ajatempli usaldus)?

2.5 Salastatud vs avalik võrk: Nortal mainib, aga lahendusklass (CDS/guard) on puudu

Nortal eeldab, et osa komponente on salastatud võrgus ja tuleb testida side avaliku/salastatud võrgu vahel.

NORTAL

Meie varasem jutt rääkis masking/obfuscation’ist, kuid siin on reaalselt vaja **cross-domain** mustreid.

Mida eelanalüüsis tõstatada:

- Kas “valge-punane” jaotus lahendatakse *andmete downgrade’iga* (policy-based field redaction) või *füüsilise CDS/guard’iga*?
- Millised objektid üldse tohivad ületada domeeni (fused track without sensor origin, coverage heatmap, alerts only)?

2.6 Standardite nimekiri on hea, kuid “meie detailne protokollipakk” on Nortali tekstis hetkel liiga üldine

Nortal ütleb “lisaks georuumi- ja ajastandardid, küberturvalisuse ja logimise standardid jt”, kuid ei too välja konkreetseid “wire-level” valikuid.

NORTAL

Meie varasem arutelu läks väga konkreetseks (PTP, multicast, syslog TLS, video transport, RF streaming jne).

Mida eelanalüüsis tõstatada:

- Eelanalüusi väljund peab sisaldama *konkreetseid* standardeid per modality + “min field set” + “adapter contract”.
- Muidu detailanalüusi/hanke faasis hakkab iga pakkaja pakkuma “oma API-d”.

2.7 “Eelistatud Eestis või lähiregioonis” vs “maksimaalne turuvalik”

Nortali põhimõte: eelistatud süsteemid, mis on Eestis või lähiregioonis, et kriisis oleks parandatavus ja tarnerisk madalam.

NORTAL

See on strateegiliselt mõistetav, aga võib hankes olla **küsิตав** ja võib **vähendada valikut**.

Mida eelanalüüsis tõstatada:

- Sõnastada see pigem “**hooldatavus / kohalik tugi / SLA / escrow**” nõudena, mitte geograafilise päritolu piiranguna.

3) Nortali plaanis on “vaikimisi puudu” mitu asja, mida meie jutus pidasime kriitiliseks

Need on head “tõstame eelanalüusi peatükkidesse / riskide nimekirja” punktid.

3.1 Ajastuse ja korrelatsiooni inseneeria (PTP / timestamp semantics)

Nortal räägib standarditest üldiselt, kuid **ajastuse** osa (PTP, timestampide tähdus, “time-of-validity”) ei ole nende lõigus konkreetselt lahti kirjutatud. Samas nad ütlevad, et andmemaht ja sagedus hinnatakse.

NORTAL

Tõstata: “kuidas tagame sensorite ajasünkrooni ja kuidas COP käsitleb hilinenud andmeid”.

3.2 Multicast / suurte voogude skaaleerimine (FMV, radar video)

PPA nõuded ütlevad “reaalaja vaade, GIS, operaator reageerib alarmidele”.

Eelanalüüs

Aga kui lisandub FMV/radar video, tuleb otsustada *kas ja kuidas* seda jagada (kellele, millises resolutsioonis, mis protokolliga). Nortali plaan ei sisalda veel konkreetset lahendusmustrit.

Tõstata: “milline on video ja radar-video jaotusmudel (unicast broker vs multicast), ja kuidas see sobib sisevõrgu piirangusse”.

3.3 Adapterite/pluginate testimine ja versioonihaldus (contract tests)

Nortal räägib “integratsionivajaduste kaardistus” ja “prototüubi vajaduse määratlemine”.

NORTAL

Aga eelanalüüs isas tasub kohe sisse tuua *praktikas kõige valusam*: “vendor muudab firmware’i → ingest murdub”.

Tõstata: “adapterite lepingu-testid, golden capture replay, versioonipoliitika ja CI”.

3.4 Evidence / menetlus: “mida kasutaja nägi” + poliitikad + downgrade otsused

Nortal õigusosa on tugev (logimine, auditeeritavus, töendatavus).

NORTAL

Aga tehniliselt tasub tõstatada: audit pole ainult “user clicked X” – vaid ka “milline andmeväljade maskimine rakendus”.

Tõstata: “policy decision logging” + “view receipts” (kellele millised väljad).

3.5 Remote ID trust (ASTM/DRIP) kui eraldi “trust plane”

PPA turu-uuring ütleb RemotID vastuvõtjad on plaanis.

Eelanalüüs

Nortali standardite loendis ei paista Remote ID / trust kihistus konkreetsest välja (vähemalt väljavõttes).

NORTAL

Tõstata: Remote ID ei ole “lihtsalt veel üks sensor” – see vajab spoofingu käsitlust ja trust verdict’i mudelit.

4) Konkreetne “mida eelanalüüs küsida / otsustada” nimekiri

Kui sa tahad eelanalüüsi dokumendis kohe “paika lüüa” asjad, mis muidu jäävad hiljem vaidluseks, siis need küsimused on kullafond:

- 1. Kas “x-tee laadne” tähendab tehnoloogiat või põhimõtet?** Kui põhimõte, siis sõnastada see “zero trust + identiteet + store-and-forward” ilma X-tee lukustuseta.

NORTAL

- 2. Milline osa liiklusest peab olema allkirjastatud?** (juhtimine/audit vs stream). Vältida nõuet “kõik liiklus allkirjastatud”.

NORTAL

- 3. Edge'i roll:** kas edge on “adapter/gateway” (normaliseerib) või “classifier” (otsustab)? Klassifikatsioon teha optional.

NORTAL

- 4. Hajus COP režiim:** regionalne “täis” vs “degradeeritud”. Replikatsioon ja “tõe allikas” otsus.

NORTAL

- 5. Salastatud/avalik liides:** kas läbi CDS/guard või läbi policy-based downgrade'i? Mis väljad tohivad üle minna?

NORTAL

- 6. Standardid per modality:** eelanalüüsi väljundis peab olema iga sensortüübi “min. fields + protokollivariandid + adapter contract”. Nortal küll loetleb standardite kategooriad, aga vajab konkretiseerimist.

NORTAL

NORTAL

- 7. Hankepoliitika “lähiregioon”:** sõnastada ümber hooldatavuse/SLA/escrow'ks, et mitte vähendada valikut.

NORTAL

- 8. Operaatorimodel:** PPA ütleb, et operaator jõuab reageerida ainult alarmidele.

Eelanalüüs

→ Eelanalüüs peab tulema “alarmide dedupe/escalation” ja “alert fatigue” käsitlus, vastasel juhul kukub kasutus läbi.

Kui tahad, võin järgmisena teha **“Eelanalüüsi peatükkide lisandused”** formaadis: ehk iga Nortali peatüki (1.2...1.7) alla konkreetne loetelu “mis küsimused/otsused sinna juurde panna”, et see oleks kooskõlas meie standardiraamistikuga ja ei tekitaks hiljem hanke ummikut.

-

1) Kuidas “X-tee laadne turvaserveritega” lahendus päriselt töötaks

Mis on “X-tee laadne” mustrina (mitte tingimata X-tee enda tehnoloogiana)

X-tee põhiidee on:

- Iga organisatsioon (asutus) hoiab **oma andmeid** ja pakub neid teistele “teenusena” (API).
- Kõik välised kutsed käivad läbi **turvaserveri** (security server / gateway), mis:
 - autentib osapooled (kes sa oled)
 - autoriseerib (kas sul on õigus)
 - **allkirjastab** (non-repudiation: hiljem saab töestada, kes mida saatis)
 - **krüpteerib** (konfidentsiaalsus)
 - logib (audit trail)
- On **registrid/konfiguratsioon**, mis ütlevad, kes on liige ja milliseid teenuseid pakub.

Kuidas see näeks välja drone COP kontekstis

Kujuta ette, et igal sensorivõrgul (või asutusel) on “EDGE sõlm”, kus on:

- sensorid + vendor adapterid
- kohalik fusion (või vähemalt normaliseerimine)

- **turvaserver/gateway**, mis on ainus “ametlik” välisiides

Andmevood 2 tüüpi:

1. **Päring-vastus (request/response)**

Näited:

- “Anna mulle viimase 10 minuti sündmused sektoris X”
- “Anna tracki ID 123 ajalugu”
- “Anna sensorite terviseseis”

2. **Push / subscription** (kui tehakse “X-tee laadseks” publish-subscribe’iks)

Näited:

- “Saada mulle kõik *alerts* ja *tracks* piirkonnast X”
- “Saada ainult abstraktne coverage/heatmap”
- “Saada ainult anonüümne track (ilma sensori päritoluta)”

Kuna klassikaline X-tee on väga tugevalt transaktsioonimudel (päring-vastus), siis reaalaegse “subscribe” jaoks peab lisama ühe nendest mustritest:

- **püsiv ühendus** (WebSocket/gRPC stream) turvaserveri kaudu
- või **broker** (AMQP/MQTT/Kafka), kuhu turvaserver avaldab ja mille kaudu tarbijad tellivad
- või “polling” (halb reaalaegseks)

Mis teeb turvaserveri siin väärthuslikuks

- **Identiteet ja usaldus:** kõik on sertifikaatidega; “kes saatis mida”
- **ABAC poliitikad:** turvaserver/edge võib enne väljastamist teha *downgrade/masking*
- **Audit:** “asutus A sai B-lt selle tracki kell 12:01, masked väljad X,Y”
- **Offline/katkestuse taluvus (kui juurde ehitada):** edge saab loksutada store-and-forward’i (queue), et kui keskne tase maas, kohalik töötab ja hiljem sünkroniseerib

Oluline nüanss: X-tee enda “central server” ei ole tavaliselt *andmete teel* (ta on registri ja konfiguratsiooni jaoks). Andmeside käib turvaserverite vahel otse. See vähendab SPOF-i, *kui* disainitud õigesti.

2) Miks multicast/streaming on meie sensorivoo jaoks tihti parem

Meie eelnev arhitektuur rääkis:

- radar video / FMV / tihe track feed = **streaming**
- “üks allikas → paljud tarbijad” = **multicast (SSM)** LAN-is
- WAN-is = **RIST/SRT** või brokerid, sõltuvalt olukorrast
- turve = **802.1X + MACsec + TLS + ABAC** maskeerimine *andmetasandil*

Multicast on “öige tööriist” körgsagedusliku telemeetria jaoks

Kui sul on näiteks:

- radar trackid 10–50 Hz
- radar video / EO video megabitid–kümned megabitid
- mitu ops-keskust + mitu vaatlejat

...siis multicast annab:

- **väga madala latentsuse**
- **väga hea skaleerimise** (allikas saadab 1x, võrk kopeerib ainult sinna, kus tellijaid on)
- **vähem serveripoolset koormust** (ei pea tegema 100 unicast streami 100 kasutajale)

X-tee laadne (eriti kui allkirjastad “iga sõnumi” ja teed per-tarbija autoriseerimist) kipub:

- muutuma “kallis CPU/latency” just kõige raskemate voogude puhul
- skaleerima halvasti, kui sama streami tahavad paljud

3) Otsene võrdlus: X-tee-laadne vs multicast (reaalne COP kontekst)

Lühike tabel

Kriteerium	X-tee-laadne turvaserver	Multicast/streaming (SSM)
Parim kasutus	päringud, sündmused, jagatud registrid, auditiga API	video, radar video, tihe telemeetria, “üks→paljud”
Reaalaegne latentsus	hea <i>kui</i> push+lightweight; halb kui “allkirjasta kõik”	väga hea LAN-is

Kriteerium	X-tee-laadne turvaserver	Multicast/streaming (SSM)
Skaleerimine 1→N	tavaliselt N unicast koopiat või broker koormus	võrk teeb kopeerimise; allikas saadab 1x
Turbe/identiteedi mudel	sisseehitatud tugev identiteet + allkiri + audit	peab eraldi tegema (802.1X/MACsec, ACL, logimine)
ABAC / maskimine	loomulik koht teha gateway's "downgrade"	peab tegema kas publisheris, brokeris või subscribe-kihis
Sobivus WAN-i	hea (API üle interneti)	multicast WAN-is tavaliselt keeruline; pigem RIST/SRT/broker
Ops keerukus	poliitikad+registrid; hästi kontrollitav	multicast nõuab head võrguoskust (IGMP/MLD/PIM)
“Kogu liikluse allkirjastus”	lihtne nõudena, raske praktikas suurvoogude jaoks	ei sobi; parem on link-krüpto + objektipõhine signatuur

“Crap moment” riskid

- X-tee laadne:** kui pannakse nõue “kõik streamid läbi turvaserveri + allkirjastatud”, siis video/radar vood muutuvad kas kalliks või hilinevaks → ops ei usalda COP-i.
- Multicast:** kui võrgu konfig on nõrk (IGMP snooping/querier), siis “töötab laboris, sureb platsil”. Või kui turve on “lõtv”, siis keegi saab valesse grupperi subscribe'ida.

4) Miks meie varasem “SSM multicast + PTP + MACsec” on COP-i *data plane*'iks tihti parem

Sinu kasutusjuht:

- palju sensoreid
- palju tarbijaid
- eriti video/radar
- pead toetama *near-real-time* otsustamist

See on klassikaline “data plane” probleem:

- vaja throughput + madal latentsus + 1→N skaleerimine

SSM multicast lahendab selle elegantsemalt kui “iga tarbija jaoks eraldi stream”.

Aga: multicast üksi ei lahenda:

- “kes nägi mida”
- “kes tohib mida”
- “kuidas maskeerida”

Need on “control plane / policy plane” mured.

5) Praktiline järeldus: parim on 2-plaani arhitektuur

Sooitus: “X-tee-laadne” *control plane’iks, multicast/streaming data plane’iks*

Control plane (turvaserver / gateway muster):

- kasutajate ja asutuste autentimine/autoriseerimine
- ABAC poliitikate otsus
- audit (kes subscribe’is, mis õigustega)
- metaandmed, query’d, ajalugu, tõendipäringud
- “subscription authorization”: turvaserver ütleb “jah/ei” + väljastab tokeni/õiguse

Data plane (multicast / RTP / ASTERIX / STANAG vood):

- radar trackid ja video (SSM)
- FMV (SSM LAN-is; WAN-is RIST/SRT)
- sensorite telemeetria (võib olla broker või gNMI)
- kõik madal-latentsuse massvoolud

Kuidas see näeb välja ühe voona

1. Kasutaja logib COP-i → saab õigused (ABAC)
2. Kui kasutaja tahab radar videot:
 - control plane teeb autoriseerimise (“võib”)
 - kui “võib”, antakse **subscription grant** (nt multicast group + source + key + policy profile)
3. Data plane’is kasutaja liitub ainult lubatud multicast group’iga

4. Audit logib: "kasutaja X tellis feed Y kell Z"

Maskeerimine:

- "valge" kasutaja saab "precise track + sensor origin"
 - "hall" kasutaja saab "track, aga sensor origin eemaldatud / koordinaadid ümardatud"
Seda saab teha:
 - kas eraldi multicast group'iga (üks on precise, teine sanitized)
 - või läbi edge gateway re-encode'iga (kallim, aga kontrollitavam)
-

6) Millal X-tee-laadne üksi võiks olla parem?

Kui süsteem oleks:

- valdavalt **madala sagedusega** (alerts, üksik sündmus)
- ilma video/radar videota
- ja fookus on "infosüsteemide integratsioonil", mitte "reaalaja sensorivoo juhtimisel"

Siis X-tee-laadne sobib rohkem.

Aga sinu COP on pigem:

- sensorivoo reaalaja platvorm + GIS + multi-user ops
 - mis tähendab, et "streaming data plane" on vältimatu.
-

7) Kuidas seda eelanalüüs is sõnastada nii, et ei lukustaks turgu

Kui eelanalüüs jäääb lause "EDGE on nagu X-tee turvaserver ja krüpteerib/allkirjastab kogu liikluse", siis hanke faasis:

- osa turust kukub ära
- ülejäänud pakuvad "oma musta kasti gateway'd"

Parem sõnastus:

- "**X-tee-laadne turvaserveri muster control plane'is**" (identiteet, poliitika, audit, autoriseeritud subscription)
- "**Multicast/streaming data plane'is**" (radar/video/tihe telemeetria)

- “Allkirjastus” = **objektipõhine** (alerts, audit-kriitilised sündmused, Remote ID trust), mitte “kõik paketid”

--

1) Milleks X-tee loodud ja milles ta on väga hea

X-tee (või “X-tee-laadne turvaserveri muster”) on eelkõige loodud:

- **asutustevaheliseks andmevahetuseks**, kus üks asutus pakub teisele **teenust** (API)
- **päring-vastus** ja “tehinguline” andmevahetus (nt “anna isiku andmed”, “kinnita päring”, “tagasta dokument”)
- tugevate nõuetega: **identiteet, autoriseerimine, logitavus, non-repudiation** (hiljem saab töestada, kes mida saatis)
- keskkonnas, kus osapooled ei usalda üksteist täielikult ja kus peab olema **audit ja vastutusahel**

X-tee on väga hea, kui:

- sõnumeid on **mõõdukas hulk**, iga sõnum on “oluline” ja vajab **jälgitavust**
- teenused on “*request/response*” või “*business transaction*”
- oluline on **andmete omaniku kontroll** (data stays where it is)
- integratsioonipind on standardiseeritud teenuste tasemel (mitte streaming)

2) Miks X-tee on *halb* või riskantne valik drone COP data-plane’iks (sensor streaming)

2.1 Disaini “DNA” on vale: X-tee = tehingud, COP = reaalaja vood

Drone COP-i “raske osa” on:

- radar video / FMV / tihe track update (kuni kümned Hz)
- “üks allikas → paljud tarbijad”

- madal latentsus, suur throughput

X-tee muster (klassikaline) eeldab:

- kontrollitud teenusekõnesid
- per-sõnum autoriseerimist ja sageli ka allkirjastamist
- “vähe, kuid tähtsad” sõnumid

Crap moment: kui sa proovid panna *kõrgsagedusliku sensorivoo* teingulise turvaserveri lähedale, tekib kas:

- latentsus + jitter (buffrid, allkirjad, policy checkid)
- CPU pudelikael
- või pead tegema nii palju erandeid, et “X-tee-laadsus” kaob ära.

2.2 “Allkirjasta kogu liiklus” on praktiliselt vale nõue

Kui X-tee tölgendus läheb suunas: “EDGE allkirjastab kogu liikluse”, siis video/radar voogude puhul on see:

- **liiga kallis** (CPU ja latentsus)
- “nonrepudiation” on streamingus harva vajalik iga paketi tasemel
- paljud sensorid ei toeta seda ega hakka toetama (turu kitsendamine)

Tulemus: hanete nõuded muutuvad selliseks, et valik väheneb ja integratsioon läheb kalliks.

2.3 1→N skaleerimine: X-tee sunnib sind unicast/broker maailma

COP-is tahavad sama feed’i:

- mitu operaatorit
- mitu keskust
- võib-olla partnerid

Multicastis: allikas saadab 1x, võrk kopeerib.

X-tee-laadses: enamasti:

- iga tarbija jaoks eraldi unicast stream (N korda koormust)
- või pead lisama brokeri (Kafka/MQTT/AMQP) ja siis X-tee roll “data plane’is” muutub segaseks.

Crap moment: üks radar feed muutub Nx koormuseks just siis, kui kriis algab ja kõik tahavad vaadata.

2.4 Operatiivne keerukus ja tõrkeotsing (“black box gateway”)

Turvaserver on hea kontrollpunkt, aga streamingus tekib tihti:

- “miks see feed viibib?” → kas gateway buffer? policy? TLS renegotiation? log server?
- “miks mõni tarbija saab ja mõni ei saa?” → subscription state + gateway state + auth state

Multicastis on ka keerukus, aga see on teistsugune (IGMP/MLD).

X-tee-laadsega saad lisaks veel *rakenduse taseme* keerukuse ja suurema hulga “pehmeid rikkeid”.

2.5 Vendor lock-in risk (paradoksaalselt)

Kui sa ütled turule “X-tee-laadne turvaserver” *sensorivoogude jaoks*, siis:

- paljud sensorivendorid ei tee seda nativselt
- nad pakuvad “meie gateway appliance” (proprietary)
- lõpuks oled lukus gateway tootjas, mitte sensoris

Multicast + standardsed sensoriformaadid (ASTERIX/STANAG/MISB/VITA49) on turul rohkem “loomulik” ning adapterid on lihtsamad ja vahetatavad.

2.6 Reaalaja “bounded latency” vs “policy latency”

COP-i puhul on oluline, et alert/track jõuab kiiresti ja ennustatavalt.

Kui iga liigutus käib läbi policy engine’i ja turvaserveri (eriti kui see teeb downgrade), tekib:

- latentsuse varieeruvus (jitter)
- halvem “determinism”

See on just see koht, kus reaalses opsis hakatakse COP-i mitte usaldama (“see on aeglane / hilineb”).

3) Millal X-tee (või X-tee-laadne muster) võiks sobida – ja isegi olla väga hea

3.1 Control plane ja cross-agency governance

X-tee-laadne muster sobib **suurepäraselt**:

- kasutaja/asutuse identiteet ja õigused
- audit trail: kes tellis mida, kes sai mida
- poliitikad ja “downgrade decision logs”
- sensorite registrid, sertifikaadid, võtmehaldus
- päringud: “anna sündmuse raport”, “anna ajalooline track”, “anna tõendipakett”

Ehk: mitte “video paketi transport”, vaid “kuidas me otsustame ja tõestame”.

3.2 Madala sagedusega sündmused (alerts) + summary feed

Kui sa piirad X-tee kaudu liikuva info:

- ainult *alerts* (nt <1 Hz)
- ainult *fused tracks* madala update sagedusega (nt 1–2 Hz)
- ainult “coverage/heatmap” või “abstract view”

...siis X-tee-laadne võib täiesti töötada ja anda tugeva auditi/identiteedi.

3.3 Kui võrgu multicast/SSM on poliitiliselt/tehniliselt keelatud

Mõnes keskkonnas on multicast “ei” (pilv, mõni telco, mõned turvapoliitikad).

Siis on sul nagunii vaja unicast/broker lahendust, ning X-tee-laadne võib olla üks viis, kuidas asutustevaheline usaldus ja audit lahendada.

3.4 Kui prioriteet on “asutuste autonoomia” > “madala latentsuse video”

Kui tellija (poliitiline) tahab, et:

- iga asutus hoiab oma andmed enda juures
- keskus on pigem “kataloog + federatsioon”
- jagamine on pigem “vajadusel” kui “pidev reaalaja voog”

Siis X-tee-laadne sobib paremini.

4) Kuidas seda kokku võtta “vastuargumendina” hanke/eelanalüüsí keeles

Kõige tugevam argument:

X-tee on *loodud teenuste ja tehtingute jaoks* (asutustevahelised päringud, auditeeritavus, nonrepudiation), kuid COP-i kõige raskem osa on *kõrgsageduslik streaming*

(radar/video/tihedad trackid), kus X-tee-laadne “turvaserver kõikide pakettide ees” tekitab latentsuse, skaleerimisprobleemid ja turu kitsenemise.

Parim kompromiss:

Kasuta X-tee-laadset mustrit **control plane’iks** (identiteet, õigused, audit, policy), ja multicast/standard-streaming **data plane’iks** (radar/video). Nii saad mõlema tugevused ilma, et teksid “vale tööriist vale töö jaoks”.

Kui tahad, kirjutan sellest 1–2 leheküljelise “Eelanalüüs riskide ja arhitektuurivaliku põhjenduse” peatüki (ametliku stiiliga), mida saad otse lisada materjalidesse: *mis on X-tee roll, mis pole, ja miks.*

x tee on ju rohkem rakendusteks kus osapooled ei usalda üksteist ja audendi jaoks

Jah — täpselt. X-tee (ja “X-tee-laadne turvaserveri muster”) ongi *disainitud* olukordadeks, kus:

- osapooled **ei usalda üksteist täielikult** (või vähemalt ei taha seda eeldada),
- **andmeomanik tahab kontrollida**, kes ja millele ligi saab,
- vaja on **tugevat auditit** ja sageli ka **non-repudiation’it** (hiljem töestatav: *kes mida küsis ja kes mida väljastas*),
- integratsioon on peamiselt **teenuste** (API) ja **tehingute** tasemel (päring/vastus, äriprotsess).

Kui panna see meie COP konteksti, siis see “X-tee sobib usaldamatutele osapooltele” tõlgendus on õige — ja see on ka põhjus, miks see *mustrina* võib olla väga väärthuslik COP **control plane’is**.

Miks see on COP-is kasulik (õiges kohas)

COP-i multi-agentuuri maailmas on *päris* probleem:

- kes tohib mida näha (ABAC),
- kuidas maskeerida/downgrade’ida,
- kuidas hiljem töestada: “asutus A nägi seda tracki kell X, väljad Y olid varjatud”,
- kuidas jagada andmeid üle domeenide (sh salastatud→avalik) kontrollitult.

See on *täpselt* X-tee tugevus: identiteet + autoriseerimine + logimine + töendatavus.

Miks see ikkagi ei tähenda, et X-tee peaks kandma kogu sensoristreami

Siin on oluline vahe kahe “plaani” vahel:

1) Control plane (usaldus/audit/poliitika)

- “Kes sa oled?” (sertifikaadid/asutus/roll)
- “Kas sul on õigus?” (ABAC poliitika)
- “Mida me jagame ja mis kujul?” (maskimine, täpsuse vähendamine, viivitus, anonüümistus)
- “Kes mida nägi/tegi?” (audit log)
- “Anna raport / ajalugu / tõendipakett” (päringud)

→ X-tee-laadne on siin väga loogiline.

2) Data plane (reaalaja kõrgsageduslik voog)

- radar video / FMV / tihedad track-update’id
- “üks allikas → paljud tarbijad”
- nõuab madalat latentsust ja skaleerimist

→ Siin on multicast/SSM (LAN) + RIST/SRT (WAN) sageli parem tööriist.

Põhipoint: X-tee on suurepärane “usaldusvärav” ja “auditvärav”, aga kui sa teed ta kohustuslikuks *kõigi pakettide* teel (eriti video/radar), siis hakkab ta paratamatult võistlema füüsika ja throughput’iga.

Kuidas seda kõige paremini kokku siduda (**praktiline “õige disain”**)

Tüüpiline “parim mõlemast maailmast” lahendus COP-is on:

1. **X-tee-laadne turvaserver / gateway** otsustab ja logib:
 - kasutaja/asutuse õigused
 - millised feed’id on lubatud (ja mis sanitiseerimise profiiliga)
 - väljastab “subscription grant’i” (nt token või “lubatud group+source”)
2. **Data plane** kannab tegeliku voo:
 - SSM multicast grupid LAN-is (või broker/unicast seal, kus multicast pole võimalik)
 - WAN-is RIST/SRT/bonding
3. Vajadusel tehakse **2 paralleelset feed’i**:
 - “full fidelity” (ainult kõrgema õigusega)

- “sanitized” (laiem jagamine, sensor origin peidetud, täpsus piiratud)

See annab sulle:

- X-tee tüüpi audit/mitteusaldus/valitsetavus
 - ja samal ajal skaleeruva reaalaegse pildi
-