Puolustusministeriö
Försvarsministeriet
Ministry of Defence

Hallituksen esitys sotilastiedustelusta annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi

HE 104/2026 vp.

Taustaa

- Sotilastiedustelulaki tullut voimaan uutena sääntelynä kesäkuussa vuonna 2019
- Laki on toiminut hyvin sekä parantanut tiedonhankintaa ja tilannekuvaa
- Muuttunut maailman poliittinen ja turvallisuuspoliittinen tilanne
- Teknologian kehitys, jonka ajuri myös sotilaallinen
- Esitys ei liity perustuslain 10 § :n muuttamiseen

Kohteet

- Sotilastiedustelun kohteena on seuraava toiminta, jos toiminta on luonteeltaan sotilaallista:
- 1) vieraan valtion asevoimien ja niihin rinnastuvien järjestäytyneiden joukkojen toiminta ja toiminnan valmistelu;
- 2) Suomen maanpuolustukseen kohdistuva tiedustelutoiminta;
- 3) joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö;
- 4) vieraan valtion sotatarvikkeiden kehittäminen ja levittäminen;
- 5) kansainvälistä rauhaa ja turvallisuutta vakavasti uhkaava kriisi;
- 6) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta vakavasti uhkaava toiminta;
- 7) Suomen kansainvälisen avun antamisen ja kansainvälisen muun toiminnan turvallisuutta vakavasti uhkaava toiminta.
- Lisäksi sotilastiedustelun kohteena on vieraan valtion toiminta tai muu sellainen toiminta, joka vakavasti uhkaa Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja

Yleiset periaatteet

- Suhteellisuusperiaate
- Vähimmän haitan periaate
- Tarkoitussidonnaisuuden periaate
- Syrjintäkielto
- Ihmis- ja perusoikeuksien kunnioittaminen
- (Luottamusperiaate)
- (Toiminnan salassa pitäminen ohjaavana periaatteena)

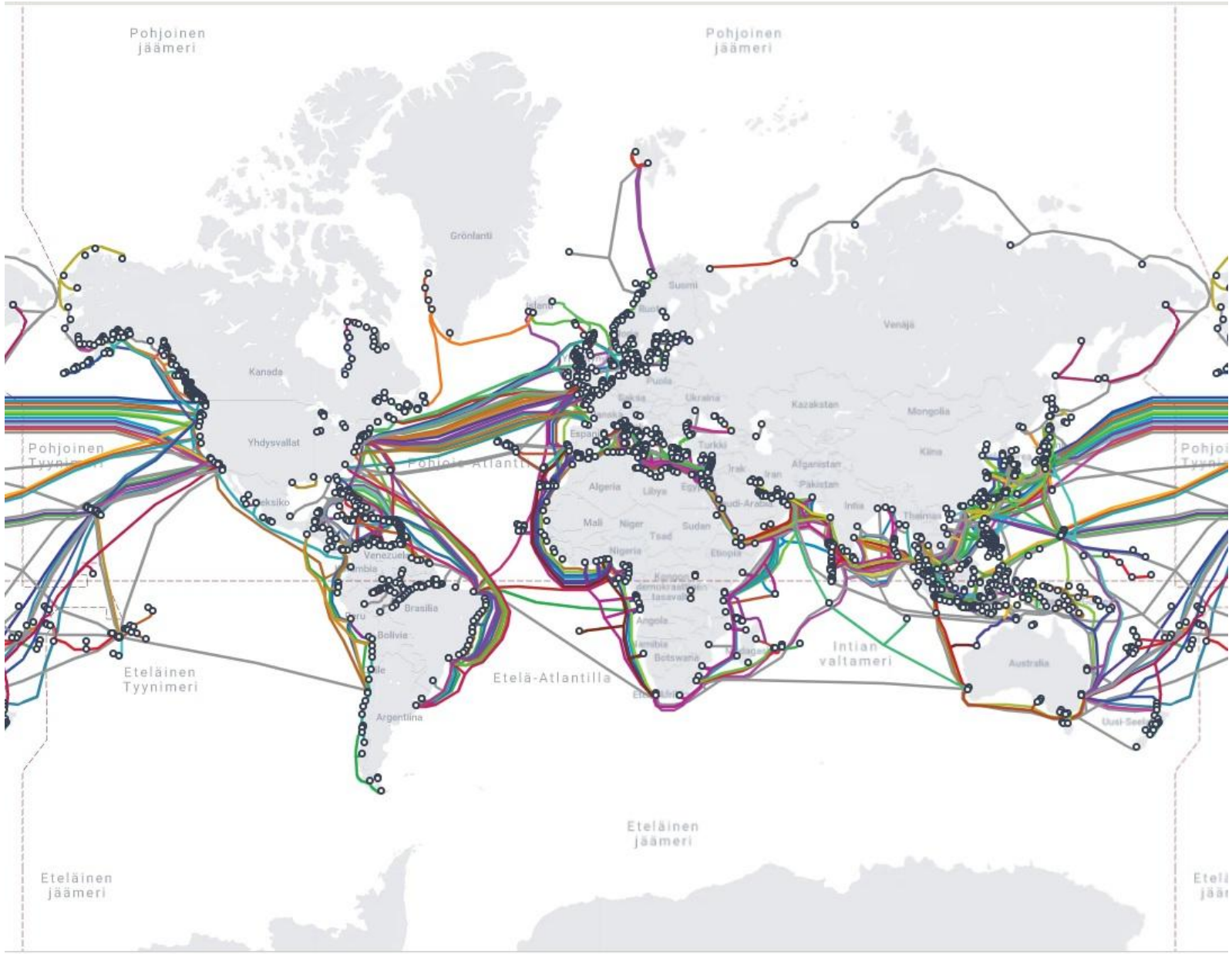
Rajoitusmekanismit

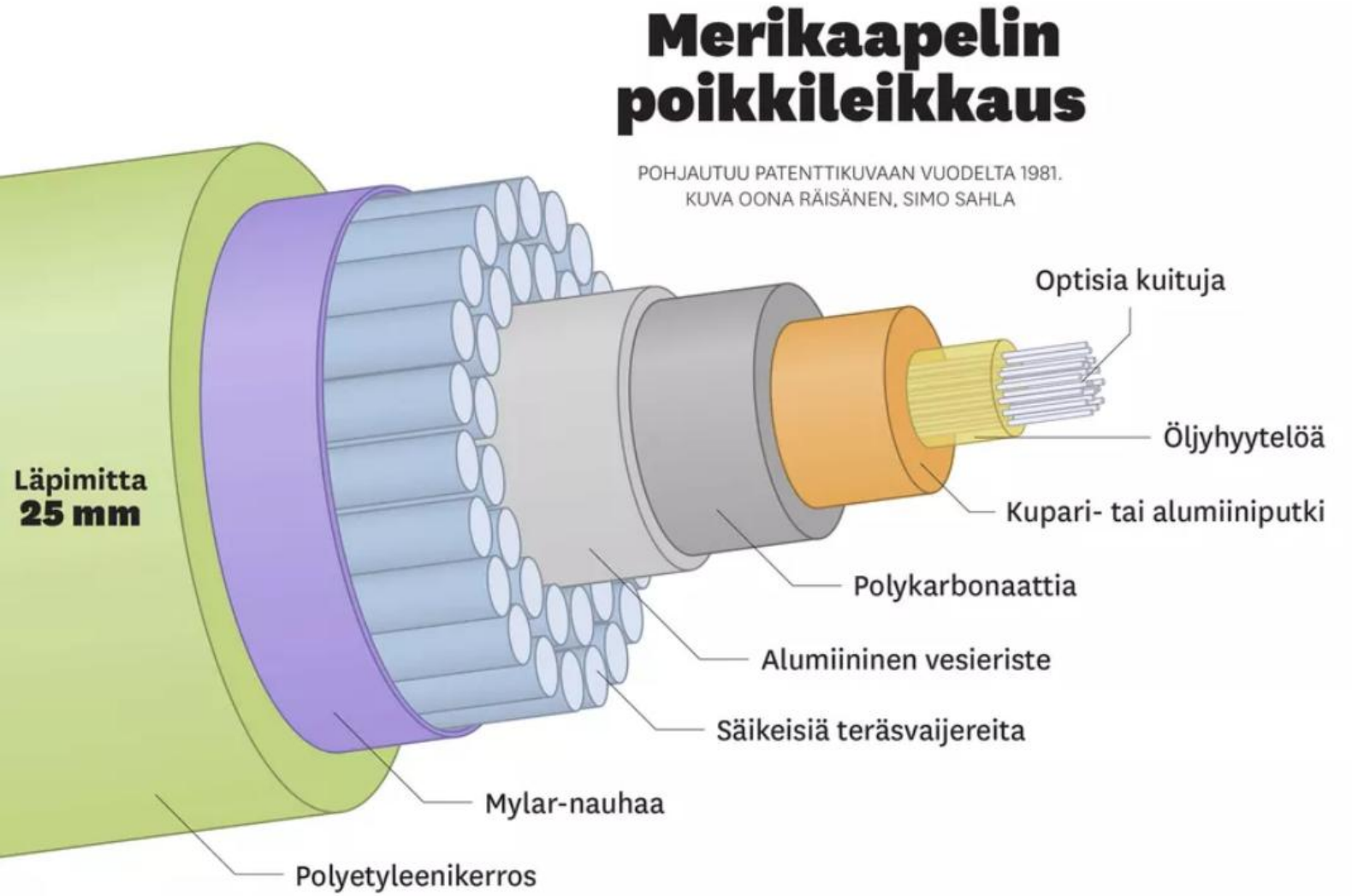
- Sotilastiedustelun kohteet
- Periaatteet
- Tiedustelutehtävä
- Hetihävittämisvelvollisuudet
- Tiedustelukiellot
- Yleiset ja erityiset edellytykset
- Tuomioistuimen päätöksenteko

Oikeusturva ja valvonta

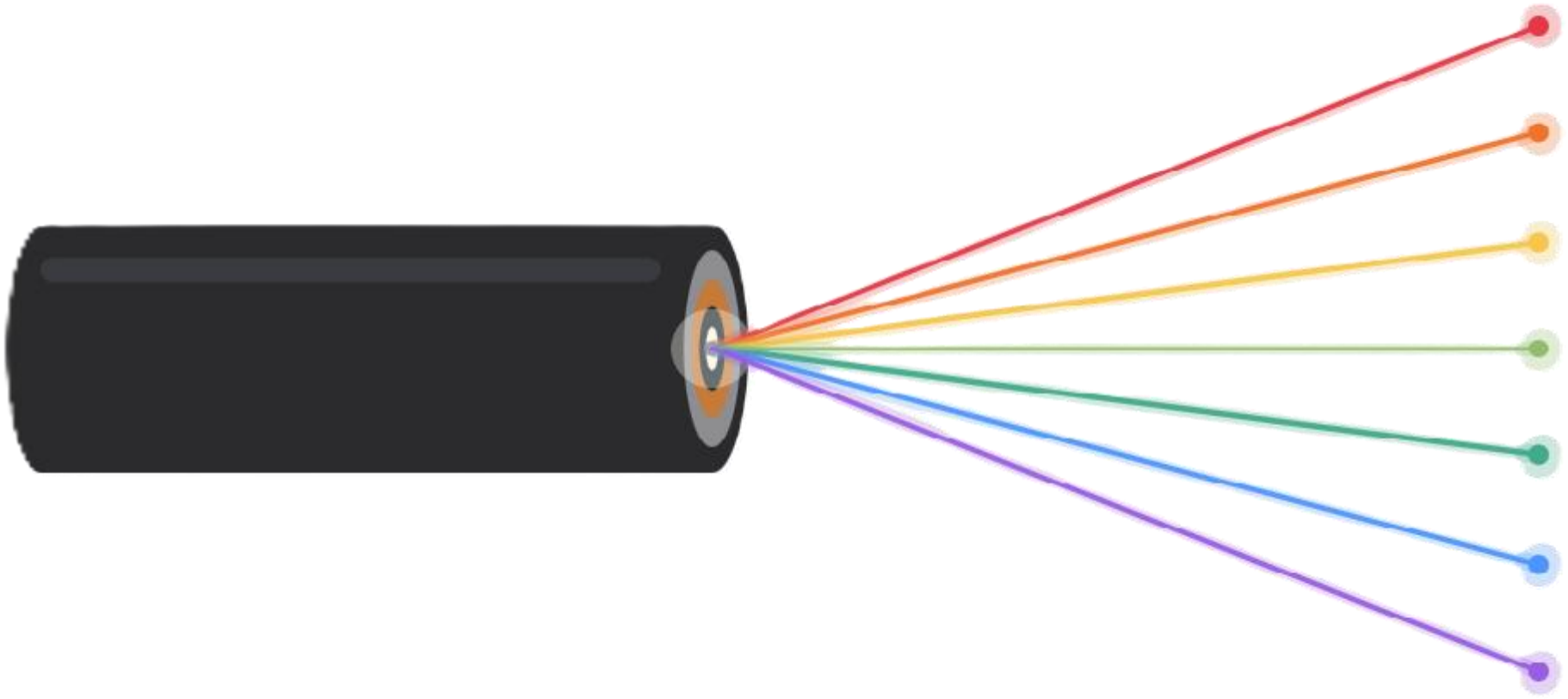
- Tuomioistuimen päätöksenteko merkittävimmissä tiedustelumenetelmissä ja kahden tuomarin kokoonpanossa
- Parlamentaarinen valvonta
- Tiedusteluvalvontavaltuutetun ennakollinen, reaaliaikainen ja jälkikäteinen valvonta
  - Kokonaisvaltaista valvontaa
  - Ennakkovalvonnassa kannanotto, voi keskeyttää tiedustelumenetelmän käytön ja saattaa asian esitutkintaan
- Eduskunnan oikeusasiamiehen valvonta, tietosuojavaltuutetun valvonta, sisäinen valvonta, ministeriön suorittama valvonta

TIETOLIIKENNETIEDUSTELU

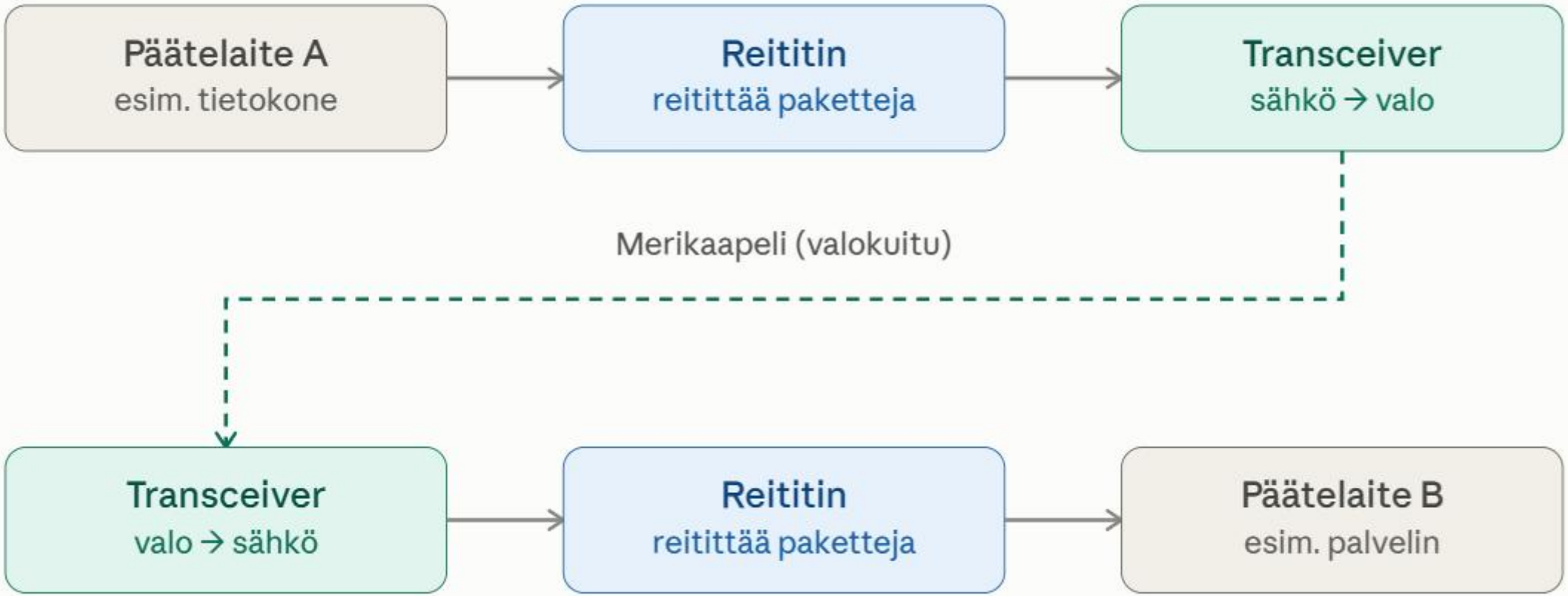

Pohjoinen jäämeri
Pohjoinen jäämeri
Grönlanti
Suomi
Venäjä
Kanada
Yhdysvallat
Kazakstan
Mongolia
Kiina
Pohjoinen Tyynimeri
Pohjois-Atlantti
Algeria
Libya
Mali
Niger
Sudan
Tsad
Nigeria
Etiopia
Afganistan
Pakistan
India
Meksiko
Venezuela
Brasilia
Bolivia
Angola
Namibia
Botswana
Etelä-Atlantilla
Intian valtameri
Australia
Eteläinen Tyynimeri
Argentiina
Eteläinen jäämeri
Eteläinen jäämeri

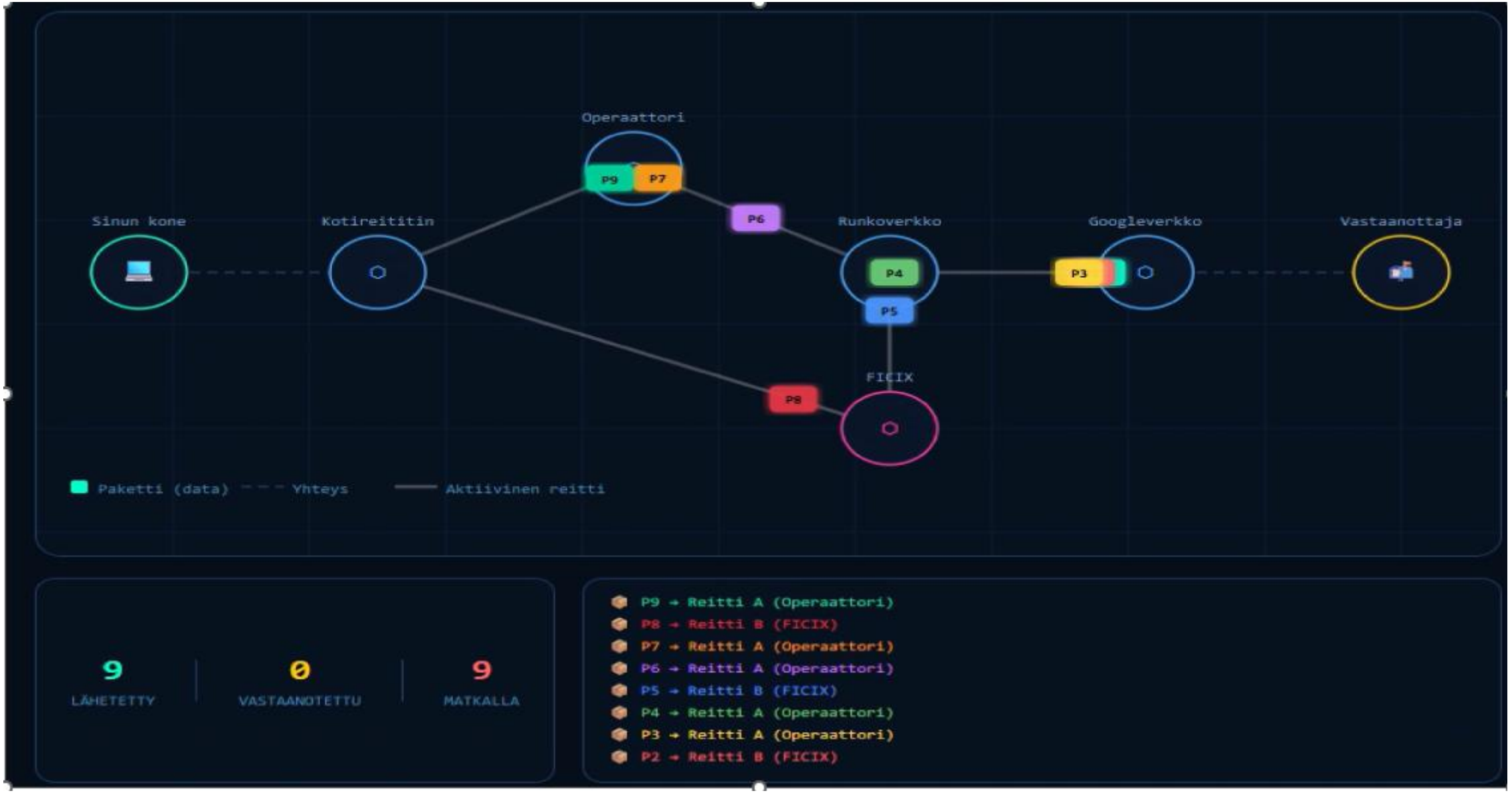


- Vanhoissa kaapeleissa kuituja oli 2-8
- Nykyisin kuituja voi olla jopa 96
- Kuituja käytetään pareissa, joista toinen tuo tietoliikennettä sisään ja toinen vie sitä ulos



- Aallonpituuksia, eli kanavia, voi olla jopa 100 per kuitu
- 400 Gt/s per aallonpituus
- Kuidun maksimikapasiteetti on siis 40 Tt/s
- Aallonpituudet infrapunavaloa eikä varsinaisia värejä voi nähdä silmin


Päätelaite A
esim. tietokone
Reititin
reitittää paketteja
Transceiver
sähkö → valo
Merikaapeli (valokuitu)
Transceiver
valo → sähkö
Reititin
reitittää paketteja
Päätelaite B
esim. palvelin


Operaattori
P9
P7
Sinun kone
Kotireititin
P6
Runkoverkko
Googleverkko
Vastaanottaja
P4
P3
P5
FICIX
P8
Paketti (data)
Yhteys
Aktiivinen reitti
9
LÄHETETTY
0
VASTAANOTETTU
9
MATKALLA
P9 → Reitti A (Operaattori)
P8 → Reitti B (FICIX)
P7 → Reitti A (Operaattori)
P6 → Reitti A (Operaattori)
P5 → Reitti B (FICIX)
P4 → Reitti A (Operaattori)
P3 → Reitti A (Operaattori)
P2 → Reitti B (FICIX)

Protokolla

- Tietoliikenteessä protokolla säännöstö, jonka avulla kaksi erilaista laitetta ymmärtävät toisiaan
  - Protokolla määrittelee esimerkiksi miten yhteys aloitetaan, missä muodossa viesti lähetetään, miten vastaanottaja kuittaa viestin vastaanotetuksi ja mitä tehdään virhetilanteissa
- Ilman yhteistä protokollaa laitteet eivät tietäisi, mitä saapuvat bitit tarkoittavat

IP PACKET STRUCTURE (IPv4)

HEADER 20-60 bytes

Version 4 bits	IHL 4 bits	DSCP 6 bits	ECN 2 bits	Total Length 16 bits	Identification 16 bits	Flags 3 bits	Fragment Offset 13 - Expires packet
Time To Live (TTL) 8 bits				Protocol Expires packet	Header Checksum 16 bits		
Source IP Address 32 bits					Destination IP Address 32 bits		Options & Padding Variable Length

PAYLOAD (DATA / UPPER LAYER PROTOCOL)

Variable Size (up to 65,535 bytes - Header)

TCP Segment
[TCP Header][Data]

UDP Datagram

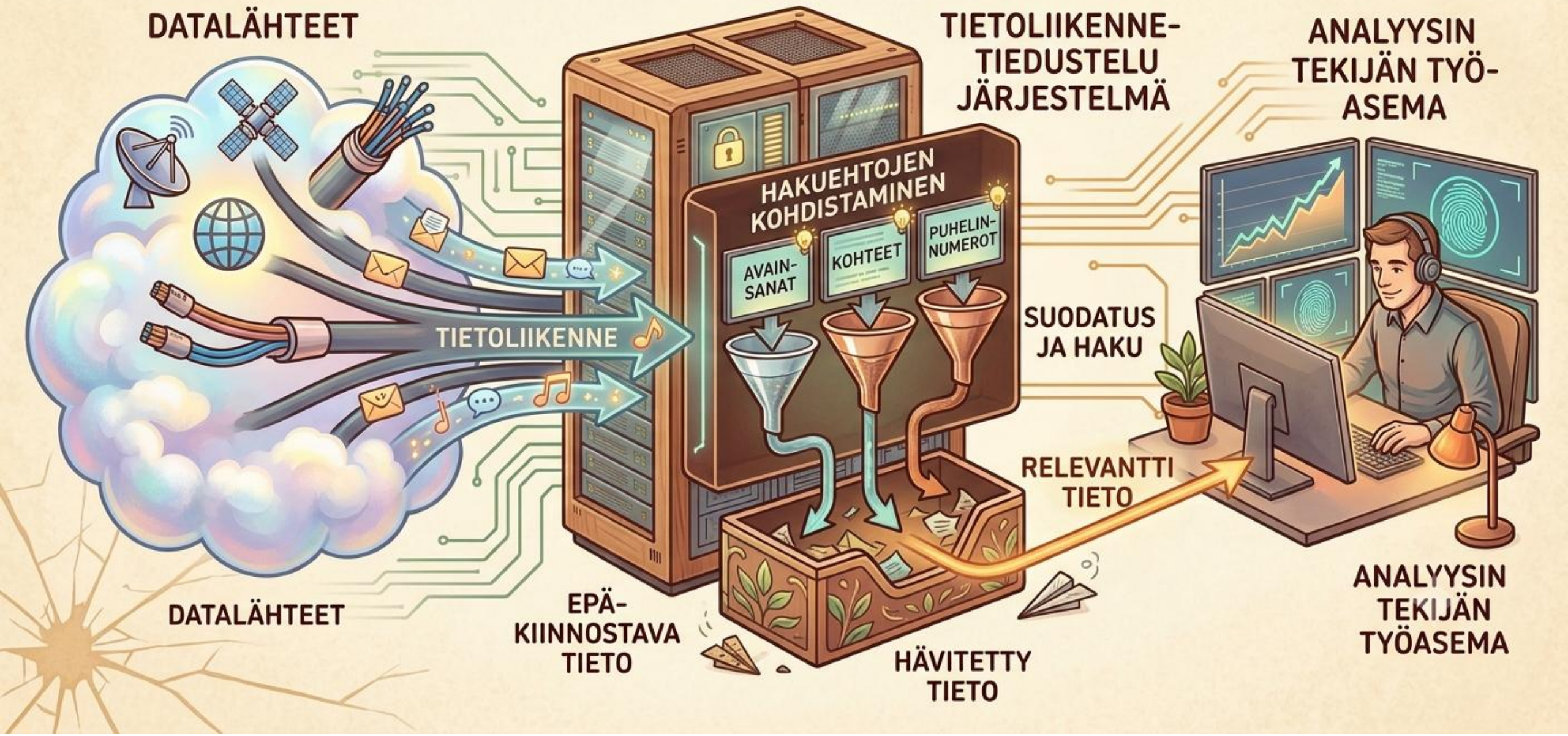
other Data

1. Header: Essential control info (20 bytes min)

2. Payload: Actual user data/message

Total IP Packet:
[Header] + [Payload]

TIETOLIIKENNE-TIEDUSTELUN PROSESSIKAAVIO



Teknisten tietojen käsittely

- Selvitetään, mihin viestintäverkon osaan varsinaista tietoliikennetiedustelua kannattaa kohdistaa
- Käsitellään tietoliikenteen teknisiä tietoja tietoliikenteen alkuperän selvittämiseksi
  - Ei selvitetä, kuka on lähettäjä tai käyttäjä taikka mitä viesti sisältää tai miksi viesti on lähetetty
- Tekninen analyysi kertoo, miten paljon eri alueilta tietoliikennettä on tullut
- Voimassa olevan lain hetkellisyydestä luovuttaisiin
  - Varmistuttu myös siitä, että järjestelmään tulee vain tietoliikenteen teknisiä tietoja

TCP/IP PROTOCOL STACK MODEL (4 LAYERS)

A simplified overview of data flow

APPLICATION LAYER

FUNCTION: USER-FACING APPLICATIONS & SERVICES



EXAMPLES:
HTTP, HTTPS, DNS, SMTP, FTP, SSH

TRANSPORT LAYER

FUNCTION: END-TO-END COMMUNICATION & DATA RELIABILITY



EXAMPLES:
TCP (Connection-oriented), UDP (Connectionless)

INTERNET LAYER

PACKET ROUTING & LOGICAL ADDRESSING



EXAMPLES:
IP (IPv4, IPv6), ICMP, ARP

NETWORK ACCESS LAYER

PHYSICAL DATA TRANSMISSION & LINKING



EXAMPLES:
Ethernet, Wi-Fi, Physical Interface, Drivers

DATA FLOW DOWN

DATA FLOW UP

RECEIVING

Hakuehtojen määrittäminen

- Tietoliikenteessä kaikki tieto muutetaan binääriseksi bittivirraksi
  - k = 01101011 o = 01101111 i = 01101001 r = 01110010
    a = 01100001
- Verkkolaitteet kuljettavat 0- ja 1-arvoja sähkö-, valo- tai radiosignaaleina paikasta toiseen ja muuttavat ne vastaanottopäässä takaisin alkuperäiseksi tiedoksi
  - Ykkösten ja nollien sarjoista laitteet ja laitteistot muodostavat viimein aistein havaittavan kuvan tai äänen
- Määrittäminen tapahtuisi tietoliikenteen konekielisessä muodossa
  - Analysoidaan 0- ja 1-lukusarjoja, joista voidaan tunnistaa kohteena olevan järjestelmän tunnusomaisia piirteitä

Hakuehtojen määrittäminen

- Tietojärjestelmillä omia ominaispiirteitään
- Puhutaan digitaalisesta jalanjäljestä
  - Joukko teknisiä ja tietojärjestelmän käyttäytymiseen liittyviä ominaisuuksia, joiden perusteella järjestelmä voidaan tunnistaa tai erottaa muista
  - Voi koostua esimerkiksi verkko- ja TLS-protokollien yksityiskohdista, DNS-käyttäytymisestä, liikennemalleista, käytetyistä sovelluksista sekä käyttöajankohdista
  - Digitaalinen jalanjälki säilyy osittain samana myös silloin, kun osoitteet, verkot tai jopa laitteet vaihtuvat

Hakuehtojen määrittäminen

- Teknologia kehittyy ja kehittämisen ajuri tällä hetkellä keskeisesti sotilaallinen
- Jo kohteena olevista tietojärjestelmistä voidaan hankkia tietoa nykyisin, koska niistä on olemassa hakuehdot
  - Hakuehtojen määritelmän mukaisesti tiedonhankinta kohdistuu tarkasti
- Nykyisin tiedonhankintaa ei voida kuitenkaan kohdistaa tunnistetun järjestelmän rinnakkaisjärjestelmän tai kohteen muun järjestelmän, joka toimii vastaavalla tavalla, tietoliikenteeseen

Hakuehtojen määrittäminen

- Määrittämisessä olennaista ei ole viestin sisältö tai tunnistetiedot, vaan missä järjestyksessä bitit liikkuvat
- Koska kohteet ovat käytännössä organisaatioita, järjestelmien tuottamassa tietoliikenteessä on toistuvaisuuksia
- Toistuvaisuuksia tunnistamalla tietoliikenteestä voidaan tunnistaa kohteita
- Tunnistetusta tietoliikenteestä voidaan tunnistaa uusia hakuehtoja
- Uusien hakuehtojen perusteella kohdennetaan varsinaista tietoliikennetiedustelua ja varsinainen tiedonhankinta alkaa

Teknisten tietojen ja konekielisen tiedon tallentaminen (EIT)

- EIT todennut päätöksissään (Rättvisa ja Big Brother Watch)

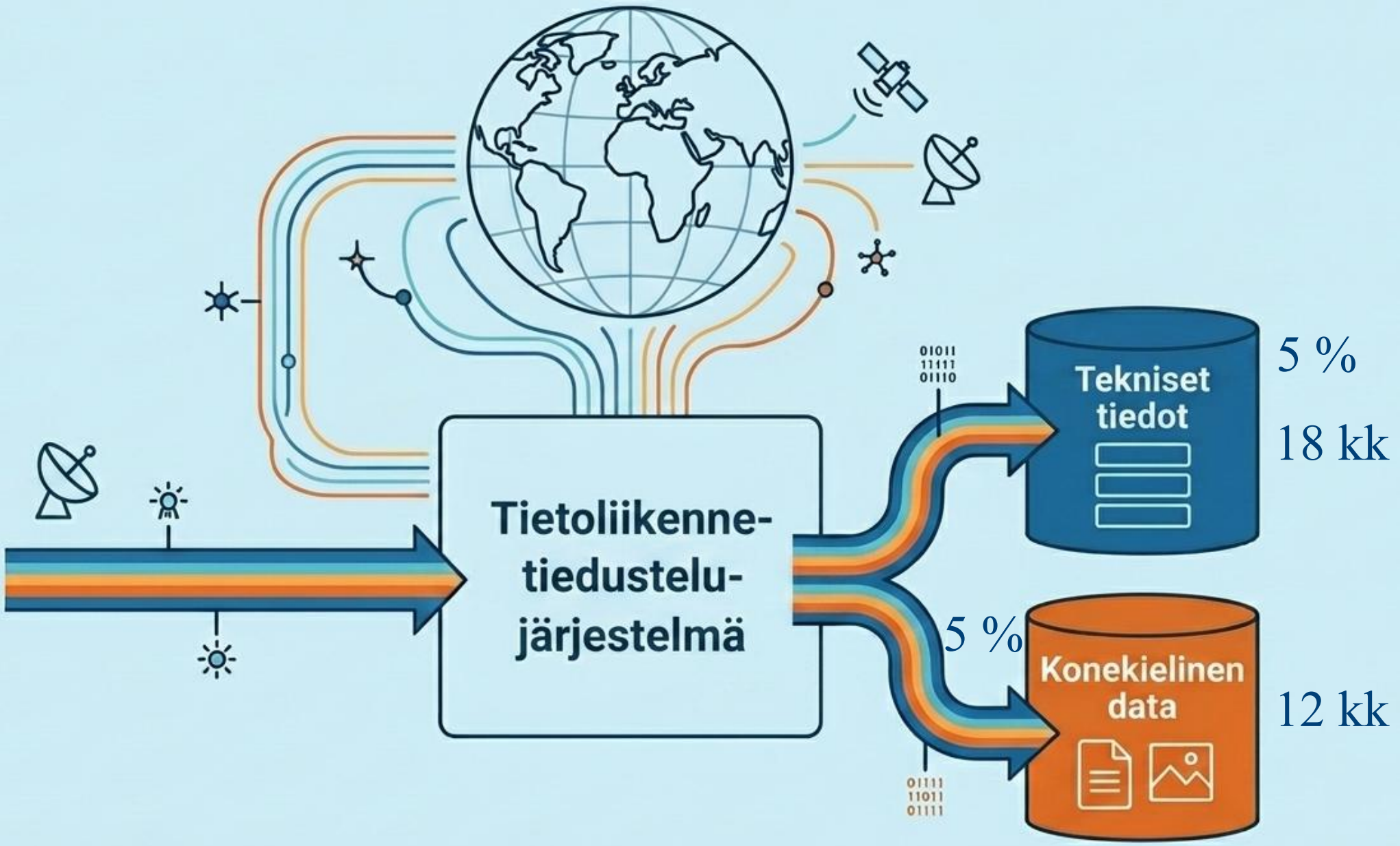
1. Tietoliikenteen hankinta ja ensivaiheen säilyttäminen
   - Viestien ja niihin liittyvien liikennetietojen kerääminen ja tallentaminen
   - EIS 8 artiklan soveltamisalassa, mutta puuttumisen intensiteetti on suhteellisen vähäinen
2. Hakuehtojen käyttäminen tietoliikenteeseen
   - Aineistoa suodatetaan esimerkiksi hakuehdoilla
   - Aineisto alkaa kohdistua tarkemmin tiettyihin viesteihin tai henkilöihin, joten yksityisyyteen puuttuminen syvenee

Teknisten tietojen ja konekielisen tiedon tallentaminen (EIT)

3. Valitun aineiston analysointi ja tutkiminen virkamiehen toimesta
    - Tiedusteluviranomainen lukee, kuuntelee tai muuten analysoi valittuja viestejä ja tietoja
    - Huomattavasti intensiivisempi puuttuminen yksityiselämään kuin pelkkä tekninen kerääminen
4. Jatkosäilyttäminen ja lopputuotteen käyttö
    - Analyysin tuloksia säilytetään, hyödynnetään tiedustelussa ja mahdollisesti jaetaan muille
    - Merkitsee itsenäistä myös puuttumista yksityisyyden suojaan

Teknisten tietojen ja konekielisen tiedon tallentaminen

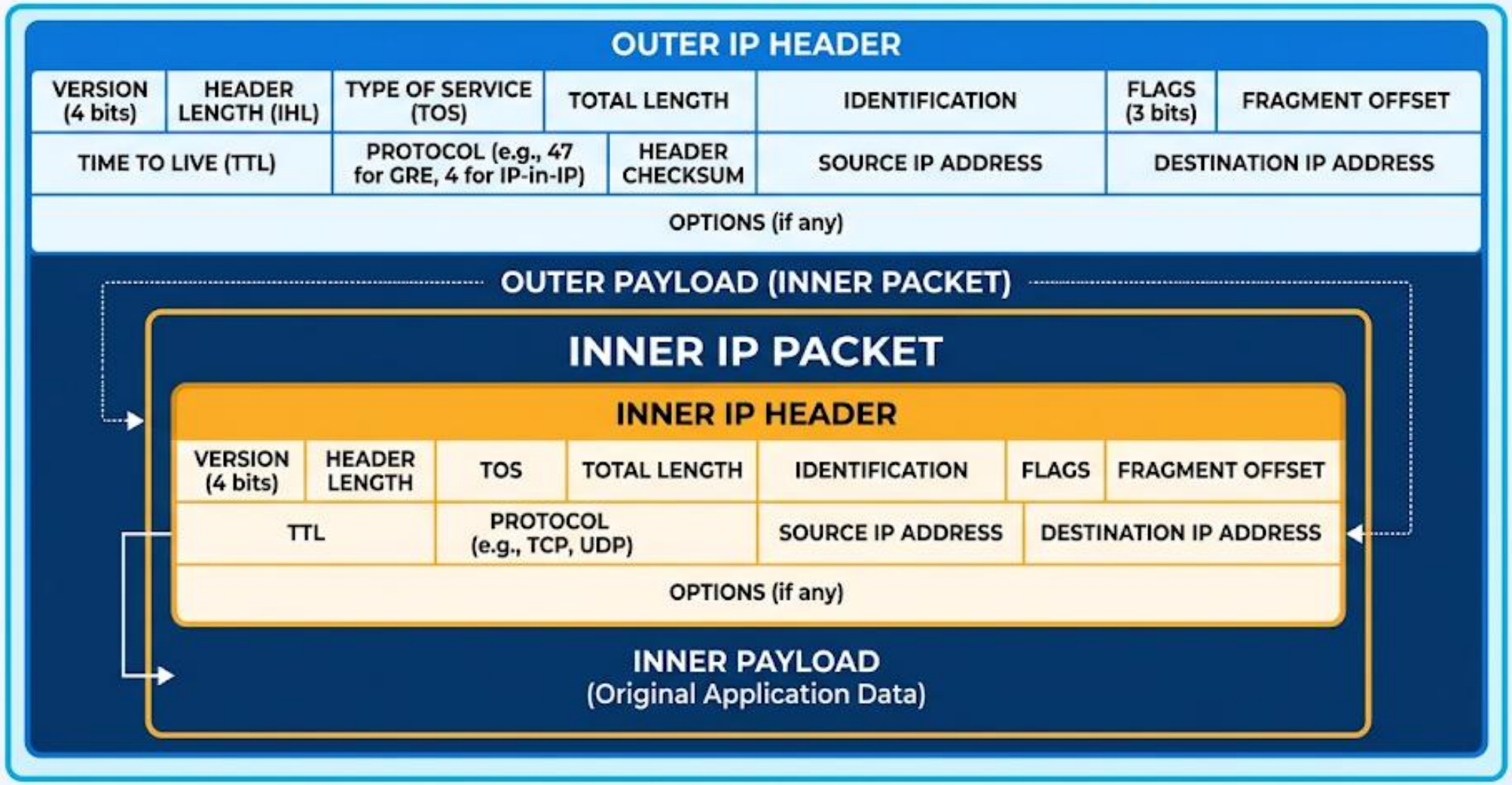
- Tallentaminen välttämätöntä tietoliikennetiedustelun tarkemmaksi kohdentamiseksi
- Operatiivinen tarve
  - Teknologia kehittyy, jonka ajuri myös sotilaallinen
- Historiatiedon avulla tunnistetaan viestintäverkossa tapahtuneita teknisiä ja tietoliikenteen reitittymisen muutoksia
  - Teknologian muutosten tunnistamisella myös vaikutusta resurssien kohdentamiseen
- Teknisiä tietoja voi tallentaa 5 % viestintäverkon osan kapasiteetista 18 kuukauden ajaksi
- Konekielistä tietovirtaa voi tallentaa 5 % kokonaiskapasiteetista 12 kuukauden ajaksi


Tietoliikenne-
tiedustelu-
järjestelmä
Tekniset
tiedot
5 %
18 kk
5 %
Konekielinen
data
12 kk

Viestin sisältöön menevä hakuehto

- Voitaisiin käyttää yhdessä muun hakuehdon kanssa
  - Nykytilassa hakuehtojen mukaista tietoliikennettä joudutaan käsittelemään laajemmin olennaisen tiedon löytämiseksi
  - Ehdotetun sääntelyn kautta jo hakuehtojen vaiheessa voitaisiin suodattaa tarpeetonta tietoa
  - Jatkokäsittelyyn päätyvä tietoliikenne olisi kohdennetumpaa
- Varsinainen viesti voi olla myös toisen viestin sisällä, jolloin varsinainen hakuehto on viestin sisällössä
- Hakuehto voi olla myös pilvipalveluun tallennettavan tiedon osana, jolloin jo nykyisin käytettävä hakuehto on viestin sisällössä

OUTER IP PACKET (ENCAPSULATED)



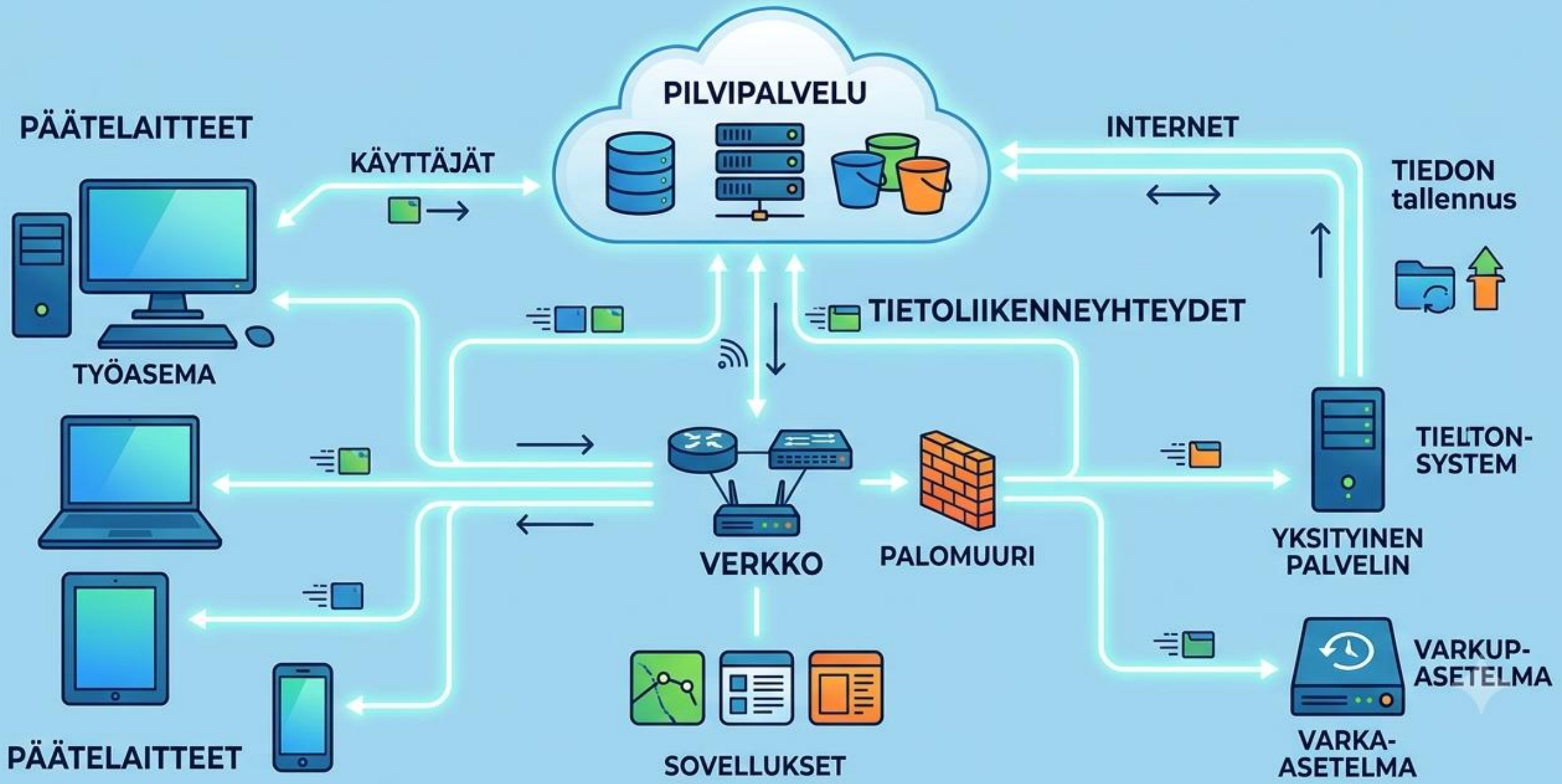
Ilmoitusvelvollisuudesta luopuminen tietoliikennetiedustelussa

- Tietoliikennetiedustelu kohdistuu ensisijaisesti tietoliikenteeseen ja kohteena olevaan toimintaan
  - Käsitellyssä voi tulla myös sivullisten tietoja
- Tehokas ilmoittaminen voi edellyttää henkilön tunnistamista ja lisätietojen hankkimista
- Voi paljastaa viranomaisen tiedustelun kohdentumista, menetelmiä ja teknisiä kykyjä sekä vaarantaa pitkäkestoisen tiedonhankinnan
- Oikeusturva ei poistuisi, vaan siirtäisi sen painopistettä tietoliinnetiedustelun erityisluonteeseen paremmin sopivaksi
  - Riippumaton, oma-aloitteinen ja koko tiedusteluketjun kattava valvonta

Kotimaan tietojärjestelmätiedustelu valtiolliseen toimijaan

- Kohdistuu kohteena olevan toimijan käyttämien laitteiden, ohjelmistojen ja yhteyksien kokonaisuuteen
  - Tiedonhankinta tapahtuu niissä rajoissa, joissa kohteena olevalla toimijalla on oikeus käyttää laitteita, ohjelmistoja ja yhteyksiä
  - Kyse ei ole rajoittamattomasta pääsystä esimerkiksi pilvipalvelun tietoihin
- Kyse osittain teknisen laitetarkkailua, televalvontaa ja telekuuntelua yhdistelevästä toimivaltuudesta

MODERNI TIETOJÄRJESTELMÄN ARKKITEHTUURI



Aktiiviset tietotekniset toimenpiteet

- Osana ulkomaan tietojärjestelmätiedustelua
  - Sotilastiedustelulla ainoastaan toimivaltuus ulkomaan tietojärjestelmätiedusteluun
- Kohteen aiheuttaessa maanpuolustukselle tai kansalliselle turvallisuudelle vakavaa uhkaa voitaisiin puuttua toiminnassa käytettävään infrastruktuuriin tai muuttaa ohjelmiston toimintaa niin, että uhka ei konkretisoidu
- Toimenpiteiden oltava suhteellisia, välttämättömiä ja väliaikaisia
  - Ei pysyvää vahinkoa omaisuudelle tai ihmisille

MODERNI TIETOJÄRJESTELMÄN ARKKITEHTUURI



Rajavartiolaitoksen osallistuminen sotilastiedustelutoimintaan

- Esityksessä ehdotetaan, että Rajavartiolaitos voisi osallistua pyynnöstä aiempaa laajemmin sotilastiedustelun avustamiseen
  - Sidottu tiettyihin toimivaltuuksiin
  - Tapahtuu sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa
  - Tehtävä siirrettävä mahdollisimman pian sotilastiedusteluviranomaiselle
  - Kyse ei virka-avusta
- Toimenpiteiden keskeyttäminen
    - Kun tehtävä siirretty sotilastiedusteluviranomaiselle tai kun sotilastiedusteluviranomainen niin käskee
    - Rajavartiolaitoksella tietojen hetihävittämisvelvollisuus

Viranomaisen ulkopuolisen osallistuminen

- Ulkopuolinen voisi suorittaa asennus- ja poisottamistoimenpiteitä
  - Esimerkiksi huoltomies, konsultti tai lähetti, jolla pääsy tiettyyn tilaa
- Viranomaisen pyynnöstä ulkopuolisen suostumuksella
- Viranomaisen ohjeistuksen mukaisesti ohjauksessa ja valvonnassa
- Toimenpiteet sotilastiedusteluviranomaisen toimivallassa
- Ulkopuolisella ei itsenäistä päätöksentekoa
- Ei käytä tiedustelumenetelmää
- Viranomaisella oltava lupa varsinaisen menetelmän käyttämiseksi

Sivullisen laitteen käyttäminen

- Mahdollista vain, jos se on välttämätöntä tiedustelumenetelmän käytön mahdollistamiseksi
  - Laite ei tiedustelun kohde, vaan tekninen väline tiedustelumenetelmän toteuttamisessa
  - Vain, jos tiedustelumenetelmän käyttöä ei voida toteuttaa muulla, sivullisen oikeuksiin vähemmän puuttuvalla tavalla
- Käyttäminen yksittäistä, lyhytaikaista ja teknisesti rajattua
  - Ei vähäistä suurempaa haittaa
- Toimenpide ei saisi vaarantaa laitteen toimintaa eikä aiheuttaa tietojen häviämistä, muuttumista tai paljastumista
- Tarkasti rajattu tekninen aputoimivalta

Ulkomaisen toimivaltaisen virkamiehen osallistuminen

- Ulkomainen toimivaltainen virkamies voisi osallistua tiedustelumenetelmän käyttöön
  - Voimassa olevan lain tietyistä toimivaltuuksista luovuttaisiin
  - Osallistuminen voisi olla kouluttamista tai varsinaisen tiedonhankintatoimenpiteen suorittaminen
- Osallistuminen tapahtuu sotilastiedusteluviranomaisen toimivallassa sekä ohjauksessa ja valvonnassa
  - Lain ja menetelmän luvan edellytysten täytyttävä
  - Tiedusteluvalvontavaltuutetun suorittama valvonta
  - Hankitut tiedot luovutetaan sotilastiedusteluviranomaiselle

Tietolähteen avustaminen Suomen rajan yli

- Tietolähteen avustamisen Suomeen tai Suomen kautta kolmanteen valtioon, jos se on välttämätöntä tietolähteen hengen tai terveyden suojaamiseksi
  - Poikkeuksellisesta ja viimesijaisesti toimesta
  - Täydentäisi viranomaisen nykyistä velvollisuutta huolehtia tietolähteen turvallisuudesta
- Ehdotus toteuttaisi perustuslain 7 ja 22 § :stä johtuvaa velvollisuutta
- Laintasoinen sääntely selkeyttäisi virkamiehen toimivaltaa ja rajanylitykseen liittyvää rikosoikeudellista vastuuta
- Käyttö edellyttää välttämättömyyttä, korkeatasoista päätöksentekoa, dokumentointia ja riippumaton valvontaa

Tiedonhankinta yleisesti saatavilla olevista lähteistä

- Selkeä lakiperusta avoimista lähteistä tapahtuvalle manuaaliselle ja automaattiselle tiedonhankinnalle
  - Avoimista lähteistä tapahtuva tehtäväsidonnainen tiedonhankinta ja sen suojaaminen laajentamatta Puolustusvoimien pääsyä ei-julkisiin tietoihin
- Rajataan Puolustusvoimien lakisääteisiin tehtäviin ja yleisesti saatavilla olevaan tietoon
- Peitteellä voidaan suojata Puolustusvoimien yhteys, tiedonhankinnan tarkoitus, menetelmän ja henkilöstön turvallisuus
- Peite ei mahdollista pääsyä ei-julkisiin tietoihin eikä muodosta itsenäistä tiedonhankintatoimivaltuutta