



**TRAFICOM**

Liikenne- ja viestintävirasto  
Kyberturvallisuuskeskus

# Kybersää

Marraskuu 2023

# #kybersää

---

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

Tämä tuote on suunnattu ensisijaisesti eri tasoilla organisaatioiden tietoturvallisuuden parissa työskenteleville.

Lukija saa nopean kokonaiskuvan, mitä kyberturvallisuuskentällä on tapahtunut ja mitä on tulossa.

**Kybersää voi olla:**



rauhallinen



huolestuttava



vakava

# Kuukauden tunnuslukuja



Kyberturvallisuuskeskukselle tehtyjen ilmoitusten perusteella Microsoft 365 -kalastelukampanjan aikana lähetettiin yli 10 000 kalasteluviestiä.<sup>[1]</sup>



Tietoturvan kehittämisen tukea myönnetty yhteensä 24 yritykselle.<sup>[2]</sup>

# Kybersää marraskuu 2023

## Tietomurrot ja -vuodot



- ▶ Tietomurtojen aiheuttamat kiristyshaittaohjelmahyökkäykset kohdentuivat erityisesti teollisuuden aloille marraskuussa. Useimmissa tapauksissa Akira- ja LockBit-kyberrikollisryhmät olivat tapausten takana.

## Huijaukset ja kalastelut



- ▶ Marraskuun alun laajalla tekstiviestikampanjalla yritettiin huijata vuokratuloja väärälle tilille.
- ▶ Facebook-sivujen haltijoita peloteltiin sivujen sulkemisella eri syistä. Huijari yritti kaapata sivut itselleen.
- ▶ Ärhäkkä pankkitunnuskalastelu pelotteli tuntemattomilla maksuilla ja tilien sulkemisella.

## Haittaohjelmat ja haavoittuvuudet



- ▶ Olemme saaneet useita ilmoituksia kiristyshaittaohjelmahavainnoista.
- ▶ Ciscon laitteissa oli useita kriittisiä haavoittuvuuksia, jotka vaativat välitöntä päivittämistä.
- ▶ Kartoitimme Citrix Bleed -haavoittuvuutta (CVE-2023-4966) ja kontaktoimme useita organisaatioita.

## Automaatio ja IoT



- ▶ EU:n kyberkestävyyssäädöksestä (CRA) saavutettiin poliittinen sopu.<sup>[3]</sup>
- ▶ Unitronicsin ohjelmoitaviin logiikkaohjaimiin (PLC) on tehty tietomurtoja myös Suomessa. Ohjaimia käytetään vedenpuhdistamoista pieniin voimalaitoksiin. Hyökkäykset ovat onnistuneet mm. heikkojen oletussalasanojen vuoksi.<sup>[4]</sup>

## Verkkojen toimivuus



- ▶ Marraskuussa yleisissä viestintäpalveluissa oli 7 merkittävää toimivuushäiriötä.
- ▶ Haktivistit kohdistivat palvelunestohyökkäyksiä Suomeen myös marraskuussa.
- ▶ Organisaatiot eivät ole raportoineet merkittävistä palveluvaikutuksista palvelunestohyökkäyksiin liittyen.

## Vakoilu



- ▶ Suojelupoliisi varoitti marraskuussa jälleen kuluttajakäyttöön tarkoitettujen verkkolaitteiden hyödyntämisestä kybervakoilussa.<sup>[5]</sup>
- ▶ Heikosti suojattuja ja haavoittuvia, internetiin yhdistettyjä laitteita murretaan osaksi hyökkäysinfrastruktuuria, ja niitä hyödyntämällä vaikeutetaan kyberhyökkäyksen havaitsemista.

# Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen



Kesästä alkaen on ollut havaittavissa kyberrikollisten nopeutunut kyky hyödyntää julki tulleita haavoittuvuuksia. Päivityksistä tulee huolehtia vuoden jokaisena päivänä, myös tulevana joulun pyhinä.



Varmuuskopioinnin muistisääntö 3 – 2 – 1. Ota vähintään 3 varmuuskopiota, säilytä niitä vähintään 2 eri formaatissa ja paikassa, sekä pidä vähintään 1 varmuuskopio irti verkosta.



Julkaisimme uuden ohjeen Tietoturva on koko organisaation asia - vinkkejä henkilöstön tietoturvakoulutuksen suunnitteluun.<sup>[6]</sup>



Tietoturvan kehittämisen tukea 24 yritykselle - enintään 100 000 euron tuet jaettiin loppuun.<sup>[2]</sup>

# Marraskuun kyberturvallisuuden yleiskuva

- ▶ Marraskuun trendeihin lukeutui tunnettujen haavoittuvuuksien hyödyntäminen tietomurroissa ja kiristyshaittaohjelmahyökkäyksissä.
  - ▶ Marraskuussa julkistettiin lukuisia kriittisiä haavoittuvuuksia, jotka edellyttivät ylläpitäjiltä välittömiä päivitys- tai rajoitustoimenpiteitä.
  - ▶ Kiristyshaittaohjelma Akiran on havaittu hyväksikäyttävän syksyistä Ciscon verkkolaittehaavoittuvuutta (CVE-2023-20269) myös Suomessa.
- ▶ Kiristyshaittaohjelmatoimijat pyrkivät usein myös salaamaan tai tuhoamaan varmuuskopiot. Tällä tavalla rikolliset vaikeuttavat merkittävästi yritysten orgaanista palautumiskykyä. Säilytä siis vähintään 1 varmuuskopio irti verkosta.
- ▶ Sähköpostitilit kuuluvat rikollisten suosikkikohteisiin. Arkaluonteiset tiedot kannattaakin lähettää salatulla sähköpostilla ja säilyttää muualla kuin sähköpostilaatikossa.

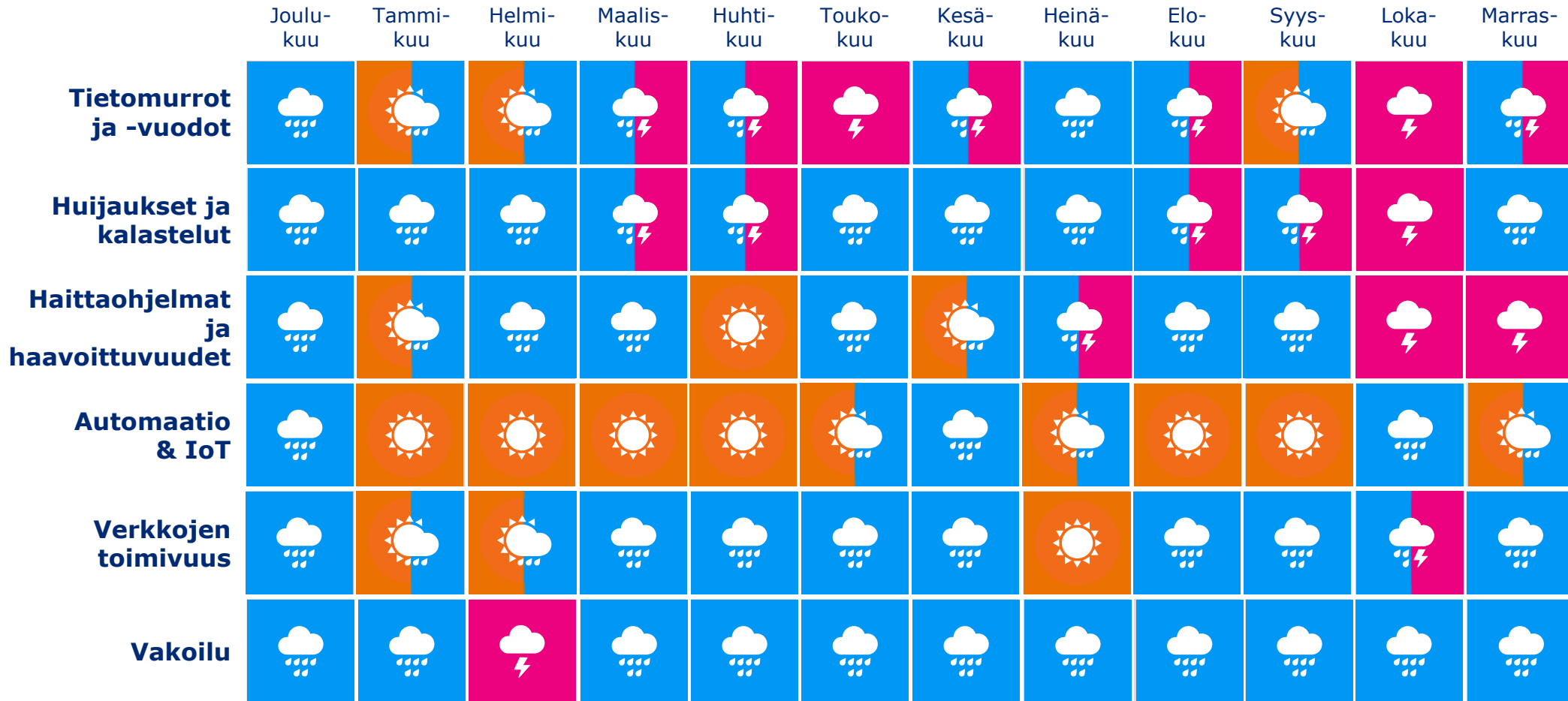
# Ilmiöiden ja toimialojen trendit

---

Osiassa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä eri aikaväleillä. Toimialakohtaisissa nostoissa on esitelty eri toimialojen tilannetta yleistasolla.



# Kyberturvallisuuden trendit kulunut 12 kk





# Pitkä aikaväli ja lähitulevaisuus

---

Osiossa on esitelty pitkän aikavälin ja lähitulevaisuuden kyberturvallisuuden ilmiöitä. Seuraamiemme pitkän aikavälin ilmiöiden joukosta analysoidaan kuukausittain yksi ilmiö. Top 5 –kyberuhkat kertovat puolestaan lähitulevaisuuden uhkista.

# Pitkän aikavälin (5v+) kybersää: ilmiöt joita seuraamme

Tarve kyber-  
turvallisuuden  
osaajille

Pula  
puolijohteista

Tekoälyn  
käyttö  
kyberrikolli-  
suudessa

Suurvalta-  
kilpailun  
vaikutukset  
sääntelyyn

Älylaitteiden  
elinkaari ja  
kierrätys

Kyber-  
vakoilun ja  
rikollisuuden  
rajojen  
hämärtymi-  
nen

**IoT**

**6G**

Kiristyshaitta-  
ohjelmien  
käyttö  
murroksessa

Teknologia  
osana  
suurvalta-  
kilpailua

Sääntelyn  
ulottuminen  
uusille  
toimialoille

Osallistu-  
minen  
digitaalisessa  
ympäristössä



# Pitkän aikavälin kybersää: 6G

**6G-matkaviestinteknologiaa kehitetään parhaillaan globaalisti, ja sitä odotetaan käyttöön 2030-luvulla. Suomessa on aloitettu 6G-tutkimus jo yli viisi vuotta sitten Oulun yliopiston koordinoimassa 6G-lippulaivahankkeessa ensimmäisten joukossa maailmassa. Suomessa halutaankin olla 6G:n osalta edelläkävijöiden joukossa.** [\[7, 8\]](#)

- ▶ Tulevaisuudessa älylaitteiden kirjo kasvaa entisestään: yhä useammat erilaiset laitteet liittyvät tulevaisuudessa pilveen tekoälyn optimoiman verkon kautta. 6G:n kaikenkattavat periaatteet ovat kestävyys, turvallisuus/yksityisyys/resilienssi, kaikkialla läsnä oleva älykkyys sekä yhteyksien tuominen kaikille. [\[8, 9\]](#)
- ▶ 6G tehostaa verkkojen hajautusta ja reunalaskennan hyödyntämistä, sekä tuo mukanaan uudentyyppisiä päätelaitteita. 6G yhdistää fyysisen, digitaalisen ja biologisen maailman ja tulee mahdollistamaan täysin uudenlaisten palvelujen kehittämisen. [\[8\]](#)
- ▶ Kansainvälinen televiestintäliitto ITU hyväksyi 6G:n (IMT-2030) viitekehyksen marraskuussa. Lisäksi EU:n Radiotaajuuspolitiikkaryhmän 6G-kannanotto on myös julkaistu. Maailman radioviestintäkonferenssissa (WRC-23) tehdään päätöksiä uusiin 6G-taajuuksiin liittyen. Traficom vaikuttaa aktiivisesti kansainvälisessä 6G-työssä. [\[10, 11\]](#)

# Tietoturva-alan kehitys, sääntely ja standardit

---

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.



## Oikeudelliset asiat

- ▶ Liikenne- ja viestintävirasto Traficomien määräys kampittaa rikollisten mahdollisuuksia tekstiviestihuijauksiin – organisaatiot voivat hakea lähettäjätunnuksensa suojausta 9.11.2023 alkaen. [\[12, 13\]](#)
- ▶ Traficomien 9.11.2023 voimaantullut määräys rajoittaa rikollisten mahdollisuutta väärentää tekstiviestin vastaanottajalle näkyvää lähettäjätietoa.
  - ▶ Määräyksen myötä organisaatiot voivat suojata käyttämänsä lähettäjätunnukset (SMS Sender ID) tiettyjen reunaehtojen puitteissa ja varmistaa, ettei mikään muu taho voi käyttää samaa tunnusta Suomessa.
  - ▶ Määräys tarjoaa tekstiviestejä lähettäville organisaatioille työkalut tunnusten suojaamiseen, mutta se ei tuo suojaa ennen kuin tunnukset on rekisteröity.
  - ▶ Hakemukset lähettäjätunnusten suojaamisesta tehdään Traficomien verkkosivuilla olevalla lomakkeella.
  - ▶ Lisäksi Traficom on julkaissut ohjeen tekstiviestin lähettäjätiedon suojaamisesta.



## Oikeudelliset asiat

- ▶ Liikenne- ja viestintävirasto Traficom in luonnos määräykseksi teletoiminnan tietoturvasta lausuntokierroksella 12.1.2024 saakka.<sup>[14]</sup>
- ▶ Määräyksellä ajantasaistetaan 4.3.2015 voimaan tullut määräys teletoiminnan tietoturvasta (Viestintävirasto 67 A/2015 M).
  - ▶ Määräys ajantasaistaa tietoturvavaatimuksia kaikkien viestintäverkkojen ja -palvelujen osalta. Määräyksessä otetaan huomioon erityisesti 5G-tekniologian uudet arkkitehtuuriratkaisut, matkaviestinverkkojen uudet käyttötapaukset ja niihin liittyvät tietoturvavaatimukset.
  - ▶ Määräyksessä määritellään tietoturvan toteuttamista koskevat vähimmäisvaatimukset. Määräyksellä pyritään siihen, että tietoturvan huomioiminen teleyrityksissä on osa jokapäiväistä toimintaa, ja että tietoturvatekijät huomioimaan rutiininomaisesti ja tehokkailla prosesseilla osana viestintäverkkojen ja -palvelujen toteutusta.
  - ▶ Määräyksen on tarkoitus tulla voimaan alkuvuodesta 2024 niin, että se tulee voimaan kolmen kuukauden kuluttua määräyksen antamisesta.



## Oikeudelliset asiat

- ▶ Euroopan parlamentti ja neuvosto ovat hyväksyneet EU:n datasäädöksen.[\[15, 16, 17\]](#)
- ▶ Euroopan neuvosto on 27.11.2023 hyväksynyt uuden asetuksen, joka koskee datan oikeudenmukaisen saatavuuden ja käytön yhdenmukaisia sääntöjä.
  - ▶ EU:n datasäädöksen tavoitteena on edistää datan oikeudenmukaista jakautumista datatalouden toimijoiden kesken, edistää datamarkkinoiden kilpailukykyä, avata mahdollisuuksia datavetoisille innovaatioille ja parantaa datan saatavuutta kaikille.
  - ▶ Datasäädöksessä asetetaan valmistajille ja palveluntarjoajille velvollisuus antaa verkkoon liitettyjen tuotteiden ja niihin liittyvien palveluiden käyttäjille pääsy ja mahdollisuus käyttää uudelleen tuotteidensa ja palvelujensa käytön tuloksena tuotettua dataa.
  - ▶ Asetus tulee voimaan 20 päivän kuluttua julkaisemisesta EU:n virallisessa lehdessä ja sitä aletaan soveltaa pääosin 20 kuukauden kuluttua voimaantulosta.



## Oikeudelliset asiat

- ▶ Euroopan tietosuojaneuvosto on julkaissut ohjeluonnoksen sähköisen viestinnän tietosuojadirektiivin (ns. ePrivacy-direktiivin) teknisestä soveltamisalasta. [\[18\]](#)
  - ▶ Ohje selventää, mitä teknisiä toimia, erityisesti uusia seurantatekniikoita, direktiivin 5 artiklan 3 kohta koskee.
  - ▶ Ohje keskittyy erityisesti uusiin ja kehitteillä oleviin seurantatekniikoihin ja siihen sisältyy käytännön esimerkkejä yleisistä seurantateknologioista.
  - ▶ Artiklan soveltamisalan selventämiseksi ohjeessa tarkastellaan artikkelissa käytettyjä keskeisiä käsitteitä.
  - ▶ Ohjeluonnos on julkisella kuulemiskierroksella 28.12.2023 saakka.





## Oikeudelliset asiat

- ▶ Euroopan neuvosto ja parlamentti ovat päässeet poliittiseen yhteisymmärrykseen EU:n kyberkestävyyssäädösehdotuksesta.<sup>[19]</sup>
  - ▶ Kyberkestävyyssäädöksellä pyritään varmistamaan, että digitaalisia elementtejä sisältävät tuotteet, kuten verkkoon liitetyt kodin valvontakamerat, televisiot ja älykellot, ovat turvallisia ennen kuin ne saatetaan markkinoille.
  - ▶ Asetuksessa otetaan käyttöön EU:n laajuiset laitteisto- ja ohjelmistotuotteiden kyberturvallisuusvaatimukset.
  - ▶ Asetusta sovelletaan lähtökohtaisesti kaikkiin tuotteisiin, jotka on liitetty suoraan tai välillisesti toiseen laitteeseen tai verkkoon.
  - ▶ Alustavasti hyväksytyssä tekstissä on säilytetty komission ehdotuksen päälinja.
  - ▶ Alustavan yhteisymmärryksen jälkeen työtä jatketaan asetuksen yksityiskohtien viimeistelemiseksi ja molempien toimielinten on vielä vahvistettava koko teksti ennen virallista hyväksymistä.

# Epäiletkö tietoturvaloukkausta?

**Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä meihin.**

- ▶ Sähköinen lomake: <https://www.kyberturvallisuuskeskus.fi/fi/ilmoita>
- ▶ Sähköposti: [cert@traficom.fi](mailto:cert@traficom.fi)
- ▶ Puhelin: 0295 345 630 (arkisin klo 9-15)

Yhteiskunnan kannalta kriittisten organisaatioiden ilmoituslomake:  
<https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx>

Muissa asioissa voitte olla meihin yhteydessä osoitteessa [kyberturvallisuuskeskus@traficom.fi](mailto:kyberturvallisuuskeskus@traficom.fi)

Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti täältä:  
<https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot>

# Lähdeluettelo

- 1) Kyberturvallisuuskeskuksen viikkokatsaus - 46/2023

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-462023>

- 2) Tietoturvan kehittämisen tukea 24 yritykselle - enintään 100 000 euron tuet jaettiin loppuun

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-kehittamisen-tukea-24-yritykselle-enintaan-100-000-euron-tuet-jaettiin>

- 3) Commission welcomes political agreement on Cyber Resilience Act

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_6168](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6168)

- 4) IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>

- 5) Nämä asiat Supo toivoo sinun muistavan, kun hankit uutta verkkolaitetta <https://supo.fi/-/nama-asiat-supo-toivoo-sinun-muistavan-kun-hankit-uutta-verkkolaitetta>

- 6) Tietoturva on koko organisaation asia - vinkkejä henkilöstön tietoturvakoulutuksen suunnitteluun

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/tietoturva-koko-organisaation-asia-vinkkeja-henkiloston>

# Lähdeluettelo

- 7) 23.11.2022 5G uutisia 6G:stä ja työstä sen edistämiseksi, satelliiteista, 5G:n hyödyntämisestä terveysteknologiassa ja operaattoreiden terveiset <https://www.traficom.fi/fi/23112022-5g-uutisia-6gsta-ja-tyosta-sen-edistamiseksi-satelliiteista-5gn-hyodyntamisesta>
- 8) Suomi vahvasti mukana Euroopan 6G-taajuustyössä <https://www.traficom.fi/fi/ajankohtaista/suomi-vahvasti-mukana-euroopan-6g-taajuustyossa>
- 9) Kansainvälinen 6G-työ tuottaa tulosta <https://uutiskirje.traficom.fi/etusivu/yhteydet/kansainvalinen-6g-tyo-tuottaa-tulosta.html>
- 10) 5G Momentum uutiskirje 4/2023 <https://uutiskirjeet.traficom.fi/a/s/166242289-696394a9cb0f269dd3288a92bd2e70ea/5629325>
- 11) Maailman radioviestintäkonferenssissa tärkeää varmistaa Suomelle riittävät taajuudet <https://www.traficom.fi/fi/ajankohtaista/maailman-radioviestintakonferenssissa-tarkeaa-varmistaa-suomelle-riittavat-taajuudet>
- 12) Traficom määrää kampittaa rikollisten mahdollisuuksia tekstiviestihuijauksiin – organisaatiot voivat hakea lähettäjätunnuksensa suojausta 9.11.2023 alkaen <https://www.traficom.fi/fi/ajankohtaista/traficomin-maarays-kampittaa-rikollisten-mahdollisuuksia-tekstiviestihuijauksiin>
- 13) SMS Sender ID -tunnus <https://www.traficom.fi/fi/viestinta/laajakaista-ja-puhelin/sms-sender-id-tunnus>

# Lähdeluettelo

14) Lausuntopyyntö luonnoksesta määräykseksi teletoiminnan tietoturvasta

<https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=9b2016b9-a4a0-44d7-b160-c03fbae7de04>

15) Parliament backs plans for better access to, and use of, data <https://www.europarl.europa.eu/news/en/press-room/20231106IPR09025/parliament-backs-plans-for-better-access-to-and-use-of-data>

16) Data Act: Council adopts new law on fair access to and use of data

<https://www.consilium.europa.eu/en/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/>

17) Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (datasäädös) <https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=COM%3A2022%3A68%3AFIN>

18) EDPB provides clarity on tracking techniques covered by the ePrivacy Directive

[https://edpb.europa.eu/news/news/2023/edpb-provides-clarity-tracking-techniques-covered-eprivacy-directive\\_en](https://edpb.europa.eu/news/news/2023/edpb-provides-clarity-tracking-techniques-covered-eprivacy-directive_en)

19) Kyberresilienssisäädös: neuvosto ja parlamentti sopuun digitaalisten tuotteiden turvallisuusvaatimuksista

<https://www.consilium.europa.eu/fi/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/>