Kyberturvallisuussanasto
Cybersäkerhetsordlista
Cybersecurity Glossary

2026 | Valtion kyberturvallisuusjohtajan toimisto, liikenne- ja viestintäministeriö
Sanastokeskus ry

Sanastokeskus

LIIKENNE- JA VIESTINTÄMINISTERIÖ
KOMMUNIKATIONSMINISTERIET

KYBERTURVALLISUUSSANASTO

Cybersäkerhetsordlista

Cybersecurity Glossary

2026

Valtion kyberturvallisuusjohtajan toimisto
Liikenne- ja viestintäministeriö

Sanastokeskus ry

ISBN 978-952-243-914-7 (PDF)

Sisällysluettelo

Käsitejärjestelmäkaavioluettelo

Esipuhe

Kyberturvallisuuden termistö on viime vuosina muuttunut paljon. Yhteiskunnan digitalisoituessa ja teknologioiden kehittyessä kyberturvallisuus on laajentunut koskettamaan yhä useampia elämänalueita. Samalla on kasvanut myös tarve ajantasaisille käsitteille.

Liikenne- ja viestintäministeriöön sijoitettu valtion kyberturvallisuusjohtajan toimisto käynnisti alkuvuodesta 2025 poikkihallinnollisen sanastoprojektin, jossa päivitettiin vuonna 2018 julkaistua Kyberturvallisuuden sanastoa (TSK 52). Sanastoprojekti on samalla ollut osa Suomen kyberturvallisuusstrategian 2024–2035 toimeenpanoa.

Kokonaisturvallisuuden näkökulmasta kyberturvallisuus on kokonaisturvallisuuden toteuttamista kybertoimintaympäristössä. Uusi Kyberturvallisuussanasto vastaa muuttunutta toimintaympäristöä ja sen käsitteet ovat linjassa sekä Suomen kyberturvallisuusstrategian että Yhteiskunnan turvallisuusstrategian (2025) keskeisten käsitteiden kanssa.

Kyberturvallisuuteen liittyvien käsitteiden määrittely on olennainen osa alan kehitystä ja siitä viestimistä niin suurelle yleisölle kuin asiantuntijoiden kesken. Käsitteiden määrittelyä tarvitaan sekä kansallista että kansainvälistä viestintää varten. Uuteen Kyberturvallisuussanastoon on lisätty ajankohtaisia käsitteitä ja vanhassa sanastossa julkaistuja käsitteitä on päivitetty tarpeen mukaan. Lisäksi joitakin vanhan sanaston käsitteitä on karsittu vanhentuneina tai tarpeettomina. Kokonaisuudessaan nyt laadittu sanasto korvaa vuonna 2018 julkaistun Kyberturvallisuuden sanaston.

Sanastoprojektin keskeisenä tavoitteena on ollut kyberturvallisuuteen liittyvien peruskäsitteiden määrittely, suositettavien termien valinta ja termien käytön selkeyttäminen. Käsitteet on pyritty määrittelemään siten, että niitä voidaan käyttää yhdenmukaisesti eri yhteyksissä. Käsitteiden välisiä suhteita havainnollistetaan käsitejärjestelmäkaavioiden avulla. Lisäksi termeille annetaan vastineet ruotsin ja englannin kielellä.

Koska sanasto kuvaa kyberturvallisuutta, monet sanaston ensisijaiset termit ovat suomeksi kyber-alkuisia ja ruotsiksi ja englanniksi cyber-alkuisia. Ruotsin ja englannin kielessä on huomattavasti tavallisempaa käyttää lyhyempää termiä ilman cyber-etuliitettä (esimerkiksi incidenthantering ja incident handling) silloin, kun yhteys kybertoimintaympäristöön on muutoin termin käyttöyhteydessä selvä. Myös suomen kielessä lyhyemmät termit ilman kyber-etuliitettä ovat yleisesti käytössä ja osin myös vakiintuneempia kuin kyber-alkuiset termit. Sanaston ensisijaisena vastineena ei siis aina ole käytetyin vaan tarkin termi.

Sanaston suomenkielisissä termisuosituksissa näkyy kielenkäytön ja termistön muuttuminen. Vanhan sanaston julkaisuhetkellä monista käsitteistä käytettävät termit olivat tuttuja tietoturvan alalta, mutta sittemmin ne ovat korvautuneet erityisesti kyberturvallisuuteen liittyvillä termeillä. Osin termivalinnat heijastelevat myös muutosta siinä, kuinka käsitteiden sisältö ymmärretään, mutta joissakin tapauksissa tietoturva- ja kybertermejä käytetään synonyymisesti asiayhteydestä riippuen. Sanastossa pääpaino on kyberturvallisuuden alan termistöllä.

Englannin kielen cyber-alkuisissa termeissä kirjoitusasu vaihtelee. Monet cyber-alkuisista termeistä kirjoitetaan nykyään pääsanansa kanssa yhteen, mutta myös erikseen kirjoitettuja (tai toisinaan yhdysviivalla kytkettyjä) termejä esiintyy. Yhteen kirjoittaminen on tavallista yleisimmin käytetyissä termeissä (esimerkiksi cyberspace ja cybersecurity), kun taas harvemmin käytetyissä tai pitkissä termeissä erikseen kirjoittaminen on tavallisempaa (esimerkiksi cyber resilience) tai pääsääntöistä (esimerkiksi cyber environment, cyber espionage). Sanastossa ei ole voitu antaa yhtenäistä suositusta kaikille cyber-alkuisille termeille, vaan kunkin käsitteen kohdalla varianttien suositettavuus perustuu sanaston laatimisajan esiintyvyyteen ja ammattimaiseen kielen tajuun.

Sanasto on tarkoitettu työvälineeksi kaikille kyberturvallisuuden parissa työskenteleville. Se edistää myös julkisen hallinnon tietojen yhteentoimivuutta. Sanasto julkaistaan myös Yhteentoimivuusalustan Sanastot-työkalussa, TEPA-termipankissa sekä valtioneuvoston termipankki Valterissa.

Kyberturvallisuussanasto on valmisteltu laajassa yhteistyössä valtionhallinnon eri organisaatioiden kanssa. Sanastotyön ohjauksesta on vastannut valtion kyberturvallisuusjohtajan toimisto.

Kyberturvallisuussanaston päivittämiseen osallistuneeseen asiantuntijaryhmään ovat kuuluneet:

Tiina Tuulensuu, valtion kyberturvallisuusjohtajan toimisto, liikenne- ja viestintäministeriö, pj.
Kimmo Janhunen, oikeusministeriö
Kirsi Janhunen, valtiovarainministeriö
Jaakko Jokela, työ- ja elinkeinoministeriö
Sara Järvinen, valtioneuvoston kanslia
Tanja Karvonen, työ- ja elinkeinoministeriö
Maria Keinonen, Maanpuolustuskorkeakoulu
Karoliina Kemppainen, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus
Anne Lohtander, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus
Anna-Minna Lukkala, sisäministeriö
Jaana Merta, maa- ja metsätalousministeriö
Niko Mäkilä, valtiovarainministeriö
Tuomo Rusila, puolustusministeriö
Jukka Seppälä, valtion kyberturvallisuusjohtajan toimisto, liikenne- ja viestintäministeriö
Mika Tuikkanen, maa- ja metsätalousministeriö
Annukka Ylivaara, Turvallisuuskomitean sihteeristö
Päivi Kouki, Sanastokeskus ry, terminologi

Lisäksi työryhmään osallistui kieliasiantuntijoita valtioneuvoston kansliasta, jonka käännös- ja kielitoimiala vastasi sanaston ruotsin- ja englanninkielisestä termityöstä.

Sanastotyöhön saatiin tukea myös muutamilta asiantuntijoilta työryhmän ulkopuolelta.

Sanastohankkeen lausuntokierroksen aikana kommentteja pyydettiin julkisen Lausuntopalvelu.fi -portaalin kautta. Määräaikaan mennessä saapui yhteensä 16 lausuntoa eri viranomaisilta, järjestöiltä, organisaatioilta ja tiedeyhteisöiltä.

Sanaston rakenne ja merkinnät

Käsitteet, määritelmät ja termit

Sanaston lähtökohtana on ollut luotettavien suomenkielisten määritelmien, käsitejärjestelmien, termisuositusten ja termien ruotsin- ja englanninkielisten vastineiden tuottaminen. Siksi sanasto on laadittu systemaattisesti, terminologisten periaatteiden ja menetelmien mukaisesti, jotka on määritelty ISO/TC 37:n (International Organization for Standardization/Technical Committee 37 Language and terminology) laatimissa kansainvälisissä standardeissa.

Terminologiselle sanastotyölle on ominaista käsitekeskeisyys. Siinä missä sanakirjat tarkastelevat sanoja ja niiden merkityksiä, terminologisten sanastojen lähtökohtana ovat käsitteet ja niiden väliset suhteet.

Käsitteet ovat ihmisen mielessään muodostamia ajatusmalleja, jotka vastaavat tiettyjä todellisuuden kohteita, niin sanottuja tarkoitteita. **Tarkoitteilla** on erilaisia ominaisuuksia. Näistä ominaisuuksista muodostettuja ajatusmalleja kutsutaan käsitepiirteiksi. Käsitteen sisältö muodostuu joukosta erilaisia käsitepiirteitä, joista olennaiset ja erottavat kuvataan **määritelmän** avulla. Terminologiset määritelmät on kirjoitettu sellaiseen muotoon, että niiden avulla voidaan tunnistaa kunkin käsitteen paikka käsitejärjestelmässä. **Termit** puolestaan ovat käsitteiden nimityksiä, joiden avulla voidaan lyhyesti viitata käsitteen koko sisältöön.

Sanaston rakenne

Sanasto on ryhmitelty **aiheenmukaisesti** jäsenneltyihin lukuihin, joissa toisiinsa liittyvät käsitteet on pyritty sijoittamaan lähekkäin.

Aakkoselliset hakemistot löytyvät sanaston lopusta. Siinä käytetty numerointi viittaa käsitteen numeroon sanastossa. Hakemistoon on poimittu suositettavien ja hylättävien termien lisäksi muita hakusanoja, jotka liittyvät läheisesti tiettyyn käsitteeseen. Muut hakusanat viittaavat siihen käsitteeseen ja sen numeroon, jonka yhteydessä kyseistä termiä käsitellään.

Termitietueen rakenne

Käsitteet on esitetty numeroituina termitietueina ja pääsääntöisesti myös käsitejärjestelmiä kuvaavina kaavioina. Termitietueet ja käsitejärjestelmäkaaviot on tarkoitettu toisiaan tukeviksi esitysmuodoiksi.

Termitietueessa käsitteelle annetaan ensin **termit**. Ensimmäisenä esitetään sanaston pääkielen (eli käsiteanalyysin perustana käytetyn kielen) termit. Termien jälkeen seuraa pääsääntöisesti **määritelmä**. Määritelmä alkaa pienellä kirjaimella ja sen lopussa ei ole pistettä. Mahdolliset määritelmää täydentävät lisätiedot eli **huomautukset** on erotettu määritelmästä sisennyksellä. Huomautukset ovat normaaleja virkkeitä. Niissä voidaan esimerkiksi antaa havainnollisia esimerkkejä, lisätietoa käsitteestä tai tietoa termien käytöstä.

Kooste kaikista käsitteiden yhteydessä sanasto-osuudessa käytetyistä merkintätavoista:

Termitietueen merkintä	**Merkinnän selitys**
1	käsitteen numero; sanaston käsitteet on numeroitu juoksevasti
lihavointi	suomenkieliset termit; suositettava termi ensimmäisenä ja sen jälkeen sallittavat synonyymit
kursivoitu linkki	(määritelmässä tai huomautuksessa) kursivoitu termi viittaa sanastossa määriteltyyn käsitteeseen; termi toimii sähköisessä versiossa linkkinä
kursivoimaton linkki	(määritelmässä tai huomautuksessa) teksti toimii linkkinä sanaston ulkopuoliseen kohteeseen, kuten säädökseen tai toisen sanaston käsitteeseen
(1)	(suluissa oleva numero termin perässä) homonyymi; sanastossa on useita kirjoitusasultaan samanlaisia suositettavia tai sallittavia termejä, joilla on eri merkitys, esim. kyberturvallisuus (1) ja kyberturvallisuus (2)
mieluummin kuin: hellre än: rather than:	ei-suositettava termi; termin käyttöä ei suositeta esimerkiksi kielellisistä syistä (kuten vierasperäisyyden vuoksi)
ei: inte: not:	hylättävä termi; tarkoittaa eri asiaa kuin suositettava termi eikä sitä pitäisi käyttää tässä merkityksessä tai termi on kielenvastainen tai vanhentunut
(uudistermi)	(teksti kaarisuluissa termin perässä) termiehdotus
sv	ruotsinkieliset vastineet; suositettava termi ensimmäisenä ja sen jälkeen sallittavat synonyymit
en	englanninkieliset vastineet; suositettava termi ensimmäisenä ja sen jälkeen sallittavat synonyymit
/FI/	suomenruotsia
n	ruotsin termi on ett-sukuinen
pl	termiä käytetään monikkomuotoisena
<	termi viittaa määriteltyä käsitettä laajempaan käsitteeseen
>	termi viittaa määriteltyä käsitettä suppeampaan käsitteeseen
~	termi viittaa hieman määritellystä käsitteestä poikkeavaan käsitteeseen, mutta siitä ei kuitenkaan voi sanoa, että se olisi laajempi tai suppeampi kuin määritelty käsite
<kyberturvallisuus>	(teksti kulmasuluissa käsitteen numeron alla) ala, jolle määritelmä on rajattu tai jonka näkökulmasta määritelmä on kirjoitettu
<Nato>	(teksti kulmasuluissa termin perässä) täsmennys termin käyttöalasta tai tapauksista, joissa termiä voidaan käyttää
Käsitejärjestelmäkaavio:	viittaus yhteen tai useampaan käsitejärjestelmäkaavioon, jossa käsite esiintyy; kaavion nimi toimii sähköisessä versiossa linkkinä

Käsitejärjestelmäkaavioiden tulkinta

Käsitejärjestelmäkaaviot havainnollistavat käsitteiden välisiä suhteita ja auttavat hahmottamaan kokonaisuuksia. Sanastossa esiintyy terminologisia käsitesuhteita, joita on kuvattu UML:n (Unified Modeling Language) mukaisilla merkintätavoilla (ks. ISO 24156-1 Graphic notations for concept modelling in terminology work and its relationship with UML – Part 1: Guidelines for using UML notation in terminology work). Kaikki alla listatut käsitesuhteet eivät välttämättä esiinny tässä sanastossa. Seuraavan sivun kaaviossa on annettu esimerkkejä käsitesuhteiden kuvaamisesta.

Käsitteen merkitseminen käsitejärjestelmäkaavioon
- sanasto-osuudesta käsitteen tiedoista on poimittu kaavioon ensimmäinen suositettava termi, mahdollinen homonyymin numero kaarisuluissa ja määritelmä
- lihavoimaton termi on kaaviossa helpottamassa kaavion tulkintaa, mutta sitä ei ole määritelty sanastossa

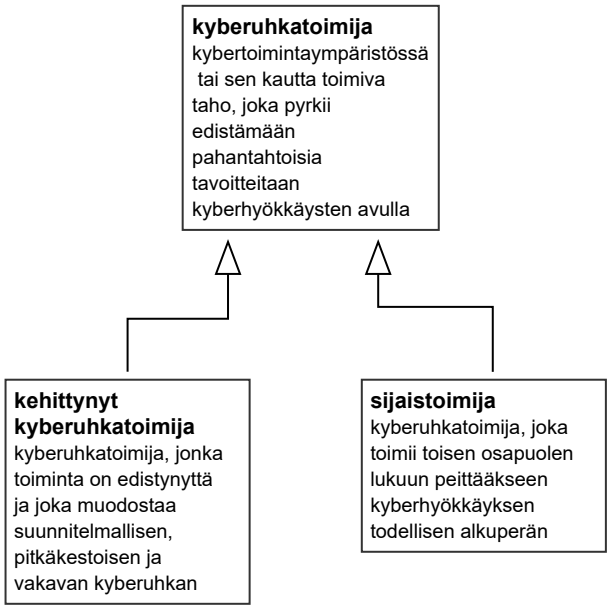
Hierarkkinen suhde (kolmioon päättyvä viiva —▷)
- vallitsee laajemman yläkäsitteen (*kyberuhkatoimija*) ja sitä suppeampien alakäsitteiden (*kehittynyt kyberuhkatoimija* ja *sijaistoimija*) välillä
- alakäsite sisältää kaikki yläkäsitteen piirteet sekä vähintään yhden lisäpiirteen, mutta sitä vastaa suppeampi joukko tarkoitteita kuin yläkäsitettä
- alakäsite voidaan ajatella yläkäsitteen erikoistapaukseksi
- kolmion kärki osoittaa yläkäsitteeseen

Koostumussuhde (vinoneliöön päättyvä viiva —◇)
- alakäsitteet ovat osia yläkäsitteenä olevasta kokonaisuudesta
- yläkäsitteen piirteet eivät sisälly alakäsitteeseen kuten hierarkkisessa käsitejärjestelmässä
- esimerkiksi *kybertoimintaympäristö* koostuu *kyberympäristöstä* ja kyberympäristöön liittyvästä toiminnasta
- vinoneliö kiinnittyy yläkäsitteeseen
- koostumussuhteen osien määrää voidaan tarvittaessa kuvata seuraavilla merkinnöillä:
  - *1..** ilmaisee sitä, että yläkäsite koostuu yhdestä tai useammasta alakäsitettä vastaavasta osasta
  - *2..** ilmaisee sitä, että yläkäsite koostuu kahdesta tai useammasta alakäsitettä vastaavasta osasta

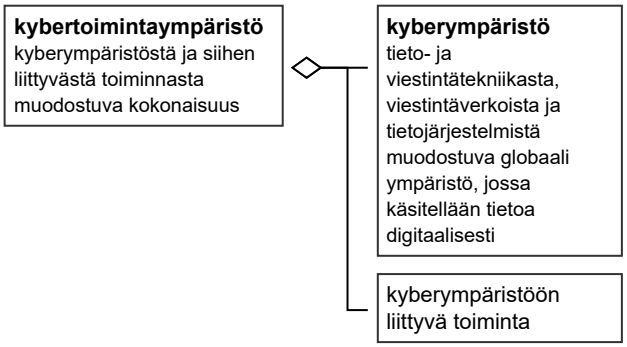
Assosiatiivinen suhde (viiva ilman symbolia)
- käsitesuhde, jota ei voida luokitella hierarkkiseksi eikä koostumussuhteeksi (esim. ajalliset, paikalliset, toiminnalliset, välineelliset sekä alkuperään ja syntyyn liittyvät suhteet)
- assosiatiivisen suhteen tyyppi käy yleensä ilmi määritelmän kielellisestä muodosta
- esimerkiksi *kyberuhkan* ja *kyberuhkanmetsästyksen* välillä on assosiatiivinen suhde: kyberuhkanmetsästys on aktiivista toimintaa kyberuhkien havaitsemiseksi

Täydentävä tieto (katkoviiva - - -)
- katkoviivoilla merkitään käsitesuhteet, jotka eivät käy ilmi määritelmien sanamuodoista (esimerkiksi käsitteiden *kyberturvallisuus (1)* ja *jatkuvuudenhallinta* välinen assosiatiivinen suhde on merkitty katkoviivalla, koska kyberturvallisuuden (1) määritelmässä ei viitata suoraan jatkuvuudenhallintaan eikä päinvastoin)
- katkoviivoilla kuvatut käsitesuhteet täydentävät määritelmiä ja tukevat käsitteiden ymmärtämistä (*jatkuvuudenhallinta* on olennainen osa *kyberturvallisuutta (1)*, vaikkei hierarkkinen käsitesuhde näy käsitteiden määritelmistä)
- katkoviivalla voidaan merkitä niin hierarkkinen suhde, koostumussuhde kuin assosiatiivinen suhdekin

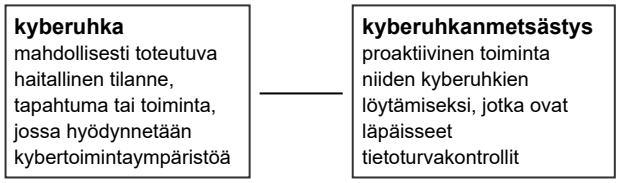
HIERARKKINENSUHDE



KOOSTUMUSSUHDE



ASSOSIATIIVINEN SUHDE



MÄÄRITELMÄÄ TÄYDENTÄVÄ KÄSITESUHDE

1 Kyberturvallisuus ja tietoturva

1

kyber-

sv cyber-

en cyber

huomautus

Kyber-sanaa käytetään yleensä yhdyssanan määriteosana. Sanan merkityssisältö liittyy usein digitaalisessa muodossa olevan informaation käsittelyyn: tietotekniikkaan, digitaaliseen viestintään (tietoverkkoihin) tai *tietojärjestelmiin*. Yleensä vasta koko yhdyssanalla (määriteosan ja perusosan yhdistelmällä) voidaan ajatella olevan oma merkityksensä.

Sanan kyber katsotaan tulevan kreikan kielen sanasta kybereo (ohjata, opastaa, hallita).

Englannin kielen cyber-alkuisissa termeissä kirjoitusasu vaihtelee. Monet cyber-alkuisista termeistä kirjoitetaan nykyään pääsanansa kanssa yhteen, mutta myös erikseen kirjoitettuja (tai toisinaan yhdysviivalla kytkettyjä) termejä esiintyy. Yhteen kirjoittaminen on tavallista yleisimmin käytetyissä termeissä (esimerkiksi cyberspace ja cybersecurity), kun taas harvemmin käytetyissä tai pitkissä termeissä erikseen kirjoittaminen on tavallisempaa (esimerkiksi cyber resilience) tai pääsääntöistä (esimerkiksi cyber espionage). Sanastossa ei ole voitu antaa yhtenäistä suositusta kaikille cyber-alkuisille termeille, vaan kunkin käsitteen kohdalla varianttien suositettavuus perustuu sanaston laatimisajan esiintyvyyteen ja ammattimaiseen kielen tajuun.

2

kyberympäristö; kyberavaruus

sv cyberrymd; cybermiljö (2)

en cyberspace

rather than: cyber environment

määritelmä

tieto- ja viestintätekniikasta, viestintäverkoista ja *tietojärjestelmistä* muodostuva globaali ympäristö, jossa käsitellään tietoa digitaalisesti

huomautus

Viestintäverkot ja tietojärjestelmät voivat olla toisiinsa liitettyjä tai toisistaan erillisiä.

Tiedon käsittelyllä tarkoitetaan tässä sen luomista, siirtämistä, muokkaamista, vaihtamista ja hyödyntämistä sen koko elinkaaren ajan.

Termien kyberympäristö ja *kybertoimintaympäristö* käyttö vaihtelee. Tässä sanastossa termeillä viitataan kahteen eri käsitteeseen, mutta toisissa yhteyksissä nämä käsitteet ymmärretään osin päällekkäisinä. Kyberympäristö ja kybertoimintaympäristö voivat joissakin tapauksissa viitata myös samaan käsitteeseen.

Termiä kyberavaruus käytetään joissakin yhteyksissä myös kybertoimintaympäristöstä.

Myös ruotsin ja englannin kielissä käsitteet voidaan ymmärtää osin päällekkäisinä ja vastineiden käyttö vaihtelee. Englanninkielinen termi cyber environment viittaa useimmiten laajempaan käsitteeseen kybertoimintaympäristö.

Käsitejärjestelmäkaaviot: Kyberturvallisuus ja tietoturva, Kyberhyökkäys, Kyberuhkat ja Kybertoimintaympäristö ja siihen liittyvä toiminta

3
kyberturvallisuus (1)
sv cybersäkerhet
en cybersecurity; cyber security

määritelmä
toimet, joilla pyritään suojaamaan viestintä- ja *tietojärjestelmät* sekä muut digitaaliset järjestelmät, niissä käsiteltävät tiedot sekä niiden käyttäjät *kyberuhkilta*

huomautus
Kyberturvallisuuteen (1) vaikuttavat olennaisesti teknologia, ihmiset ja prosessit.

Tietoturva ja kyberturvallisuus (1) ovat limittyviä ja osittain päällekkäisiä käsitteitä. Siksi on mahdotonta rajata monia niihin kuuluvia toimia yksinomaan tietoturvaan tai kyberturvallisuuteen (1) liittyviksi.

Koska kansainvälisessä viitekehyksessä, kuten EU:ssa ja Natossa, käsite cybersecurity on yleisesti määritelty toimiksi, myös tässä sanastossa on päädytty viittaamaan kyberturvallisuus-termillä toimiin. Muissa yhteyksissä termillä voidaan viitata toimien sijasta myös tavoitetilaan, jossa viestintä- ja tietojärjestelmät sekä muut digitaaliset järjestelmät, niissä käsiteltävät tiedot sekä niiden käyttäjät on suojattu kyberuhkilta.

Erityisesti Puolustusvoimien toiminnan yhteydessä käytetään myös termiä kybersuojautuminen. Sillä viitataan niihin yksilön tai joukon toimenpiteisiin, joilla suojaudutaan kyberuhkilta.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaaviot: Kyberturvallisuus ja tietoturva, Kyberuhkat ja Kybertoimintaympäristö ja siihen liittyvä toiminta

4
kyberhygienia
sv cyberhygien
en cyber hygiene

määritelmä
säännölliset ja ennakoivat toimet ja menettelyt, joilla käyttäjä tai yhteisö ylläpitää toimintaympäristönsä turvallisuutta ja osaltaan suojaa sitä *kyberuhkilta*

huomautus
Käyttäjän toimia ovat hyvät kyberhygieniakäytännöt, kuten säännöllinen salasanan vaihtaminen, päivityksistä huolehtiminen, *monivaiheisen todentamisen* käyttäminen sekä oman osaamisen ja riskitietoisuuden ylläpitäminen. Yhteisön toimiin kuuluu esimerkiksi omien *tietojärjestelmien*, laitteiden ja tietoverkkojen ja niiden kriittisten osien tunnistaminen, säännölliset päivitykset, *hyökkäyspinta-alan* pitäminen mahdollisimman pienenä, *haittaohjelmilta* suojautuminen, *pääsynhallinta*, tapahtumakirjaukset eli lokit, *kyberpoikkeamien* havainnointi ja *kyberpoikkeamanhallinta*, käyttäjien säännöllinen kouluttaminen ja ohjeiden ajantasaisuudesta huolehtiminen sekä muutoinkin hyvästä *tietoturvasta* huolehtiminen toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi.

Kyberhygienia on osa *kyberturvallisuutta (1)*.

Käsitejärjestelmäkaaviot: Kyberturvallisuus ja tietoturva ja Kybertoimintaympäristö ja siihen liittyvä toiminta

5
tietojärjestelmä
sv informationssystem *n*; datasystem *n*
en information system; data system

määritelmä
digitaalisista tiedoista, niitä käsittelevistä ohjelmista, käsittelysäännöistä, käsittelyn laiteresursseista sekä toimintaohjeista koostuva järjestelmä

huomautus
Joissakin yhteyksissä tietojärjestelmän osaksi luetaan myös niitä käyttävien ihmisten toimintakäytännöt.

Käsitejärjestelmäkaaviot: Kyberturvallisuus ja tietoturva ja Kyberhyökkäys

6
tietoturva; tietoturvallisuus
sv informationssäkerhet; > it-säkerhet; > datasäkerhet <tietoaineistoista>
en < information security; > data security <tietoaineistoista>

määritelmä
hallinnolliset ja tekniset toimet, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus

huomautus
Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Joissakin yhteyksissä tietoturvaan katsotaan kuuluvaksi myös esimerkiksi tiedon aitouden varmistaminen. Aitous tarkoittaa, että tieto on alkuperäistä, luotettavasti tunnistettavissa ja sitä ei ole muutettu luvatta.

Tietoturva on osa yhteisöjen ja käyttäjien *kyberhygieniaa* ja se suojaa *kyberympäristöä*.

Käsitejärjestelmäkaavio: Kyberturvallisuus ja tietoturva

7
tietoturvauhka
sv hot *n* mot informationssäkerheten; informationssäkerhetshot *n*
en information security threat; data security threat

määritelmä
haitallinen tapahtuma tai kehityskulku, joka kohdistuu *tietoturvaan* ja toteutuessaan vaarantaa sen

huomautus
Tietoturvauhka on usein myös *kyberuhka*. Kaikki tietoturvauhkat eivät kuitenkaan liity digitaaliseen tiedonkäsittelyyn.

Käsitejärjestelmäkaavio: Kyberturvallisuus ja tietoturva

8
tietoturvaloukkaus
sv säkerhetsöverträdelse
en data breach; < breach; < security breach; ~ data violation; ~ security violation

määritelmä
tahallinen tai tahaton teko tai laiminlyönti, joka vaarantaa *tietoturvan*

huomautus
Tietoturvaloukkauksia ovat esimerkiksi arkaluonteisten tietojen toimittaminen epähuomiossa väärälle taholle, käyttäjätunnusten ja salasanojen väärinkäyttö sekä tietojen varastaminen.

Tietoturvaloukkaus voi olla seurausta *kyberhyökkäyksestä*.

Käsitejärjestelmäkaaviot: Kyberturvallisuus ja tietoturva ja Kyberhyökkäys

9

kyberpoikkeama; kyberturvallisuuden poikkeama; < poikkeama; > kyberhäiriö

sv cyberincident; cybersäkerhetsincident; < incident; > cyberstörning

en cyber incident; cyberincident; cybersecurity incident; cyber security incident; < security incident; < incident; communication and information system security incident <Nato>

määritelmä

ei-toivottu muutos *tietojärjestelmissä* tai tietoliikenteessä, joka saattaa haitata tai vaarantaa organisaation tai järjestelmän toimintaa, palveluja tai tietoa

huomautus

Kyberpoikkeamassa ei ole kyse pelkästä teknisestä häiriöstä, vaan se voi vaikuttaa organisaation toiminnan jatkuvuuteen, *tietoturvaan* ja luottamukseen. Kyberpoikkeama voi johtua esimerkiksi siitä, että organisaation *kyberturvallisuudessa (1)*, *kyberhygieniassa* tai *jatkuvuudenhallinnassa* on puutteita. Kyberpoikkeaman syynä voi olla esimerkiksi *kyberuhkan* toteutuminen, inhimillinen tekijä tai luonnonilmiö.

Poikkeama-termillä voidaan eri säädöksissä viitata eriasteisiin kyberpoikkeamiin. Kyberturvallisuuslain (124/2025) mukaan merkittävällä poikkeamalla tarkoitetaan kyberpoikkeamaa, joka on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai huomattavia taloudellisia tappioita asianomaiselle toimijalle, sekä kyberpoikkeamaa, joka on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

Kyberhäiriö-termissä painottuu haitallinen vaikutus organisaation tai järjestelmän toimintaan.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaaviot: Kyberturvallisuus ja tietoturva ja Kybertoimintaympäristö ja siihen liittyvä toiminta

10

kyberpoikkeamanhallinta; < poikkeamanhallinta

sv cyberincidenthantering; < incidenthantering

en cyber incident handling; cyber incident response; < incident handling; < incident response

määritelmä

toimet ja menettelyt, joilla pyritään valmistautumaan *kyberpoikkeamiin*, analysoimaan, rajoittamaan ja hallitsemaan niitä sekä palautumaan ja oppimaan niistä

huomautus

Kyberpoikkeamanhallintaan voi kuulua esimerkiksi ohjelmistopäivitysten tekemistä, lokien tarkastelua ja niistä tehtyjen havaintojen luokittelua sekä kyberpoikkeamista raportointia.

Kyberpoikkeamasta riippuen kyberpoikkeamanhallinta voi edellyttää useita erilaisia toimenpiteitä ja erilaisten turvallisuusnäkökulmien varmistamista.

Ruotsin ja englannin kielissä on tavallisempaa käyttää lyhyempää termiä ilman cyber-alkua silloin, kun yhteys *kybertoimintaympäristöön* on muutoin termin käyttöyhteydessä selvä.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*. Termin cyber incident voi kirjoittaa myös yhteen.

Käsitejärjestelmäkaavio: Kyberturvallisuus ja tietoturva

11

kyberturvallisuusvalvomo; SOC; CSOC

mieluummin kuin: kyberturvakeskus

sv cybersäkerhetscenter; säkerhetsoperationscenter; SOC; CSOC

en Cyber Security Operations Centre; CSOC; Security Operations Centre; SOC

määritelmä

toiminto, joka havainnoi organisaation *kyberpoikkeamia* ja osallistuu *kyberpoikkeamanhallintaan*

huomautus

Kyberturvallisuusvalvomon toimintaan kuuluu kyberpoikkeamien vakavuuden arviointi ja niistä raportointi. Eri organisaatioissa kyberturvallisuusvalvomon tehtävät kyberpoikkeamanhallinnassa määritellään eri tavoin.

Kyberturvallisuusvalvomo voi olla organisaation oma toiminto tai valvomon palvelut voidaan ostaa ulkopuoliselta toimijalta.

Käsitejärjestelmäkaavio: Kyberturvallisuus ja tietoturva

12
CSIRT-yksikkö; CSIRT-toiminto; CSIRT
sv CSIRT-enhet; CSIRT-verksamhet; CSIRT
en Computer Security and Incident Response Team; CSIRT

määritelmä
kansallinen toiminto, jonka tehtäviin kuuluu *kybertoimintaympäristöön* kohdistuvien *tietoturvaloukkausten* ennaltaehkäisy, havainnointi ja ratkaiseminen, *kyberuhkista* ja muista *kyberturvallisuuteen (1)* liittyvistä asioista tiedottaminen sekä tiedon kerääminen

huomautus
Kansallinen CSIRT-yksikkö on Suomessa Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen tehtävä.

Lyhenne CSIRT tulee englanninkielisestä termistä computer security and incident response team. Joissakin yhteyksissä CSIRT-nimitystä käytetään myös muista toiminnoista tai yksiköistä, joiden tehtävät ovat osittain vastaavia kuin tässä kuvatut kansallisen CSIRT-yksikön tehtävät.

Käsitejärjestelmäkaavio: Kyberturvallisuus ja tietoturva

13
pääsynhallinta
sv åtkomsthantering
hellre än: accesshantering
en access management
not: ~ access control

määritelmä
menettelyt, joilla varmistetaan, että käyttäjät pääsevät käyttämään *tietojärjestelmissä* olevia tietoja käyttöoikeuksiensa mukaisesti

huomautus
Käyttäjät voivat olla ihmisiä, laitteita, tietojärjestelmiä tai ohjelmia.

Pääsynhallinta on osa *tietoturvaa*.

Englanninkielinen termi access control viittaa menettelyihin, joilla hallitaan käyttöoikeuksia.

Käsitejärjestelmäkaavio: Kyberturvallisuus ja tietoturva

14
todentaminen; todennus; ~ tunnistaminen
mieluummin kuin: autentikointi
sv autentisering; verifiering
en authentication; verification

määritelmä
menettely, jolla pyritään varmistumaan kohteen todenmukaisuudesta, oikeellisuudesta tai alkuperästä

huomautus
Kyberturvallisuuden (1) yhteydessä todentaminen liittyy usein *pääsynhallintaan* ja sillä edistetään *tietoturvaa*.

Todentamista on eri tasoista: se voi olla vahvaa tai heikkoa ja se voidaan tehdä halutulla varmuustasolla.

Kun todentamisen kohde on ihminen, käytetään usein termiä tunnistaminen.

Käsitejärjestelmäkaavio: Kyberturvallisuus ja tietoturva

15

monivaiheinen todentaminen; monivaiheinen todennus; monimenetelmäinen todentaminen; monimenetelmäinen todennus; ~ kaksivaiheinen todentaminen; ~ monivaiheinen tunnistaminen

sv multifaktorsautentisering (1); flerfaktorsautentisering; MFA; ~ tvåfaktorsautentisering; ~ tvåstegsautentisering

en multi-factor authentication; MFA; multi-step authentication; multi-factor verification; multi-step verification; ~ two-factor authentication; ~ 2FA; ~ two-step authentication; ~ multi-factor identification (1); ~ multi-step identification (1)

määritelmä

todentaminen vähintään kahta eri menetelmää käyttäen

huomautus

Silloin, kun todentaminen tehdään kahta eri menetelmää käyttäen, käytetään usein termiä kaksivaiheinen todentaminen (2FA).

Kun monivaiheisen todentamisen kohde on ihminen, käytetään usein termiä monivaiheinen tunnistaminen.

Käsitejärjestelmäkaavio: Kyberturvallisuus ja tietoturva

16

sähköinen tunnistautuminen; ~ monivaiheinen tunnistautuminen

sv elektronisk identifiering; digital identifiering; e-identifiering; ~ multifaktorsautentisering (2)

en electronic identification; e-identification; eID; digital identification; digital ID; ~ multi-factor identification (2); ~ multi-step identification (2)
rather than: online identification

määritelmä

menettely, jolla henkilö todentaa identiteettinsä digitaalisessa toimintaympäristössä

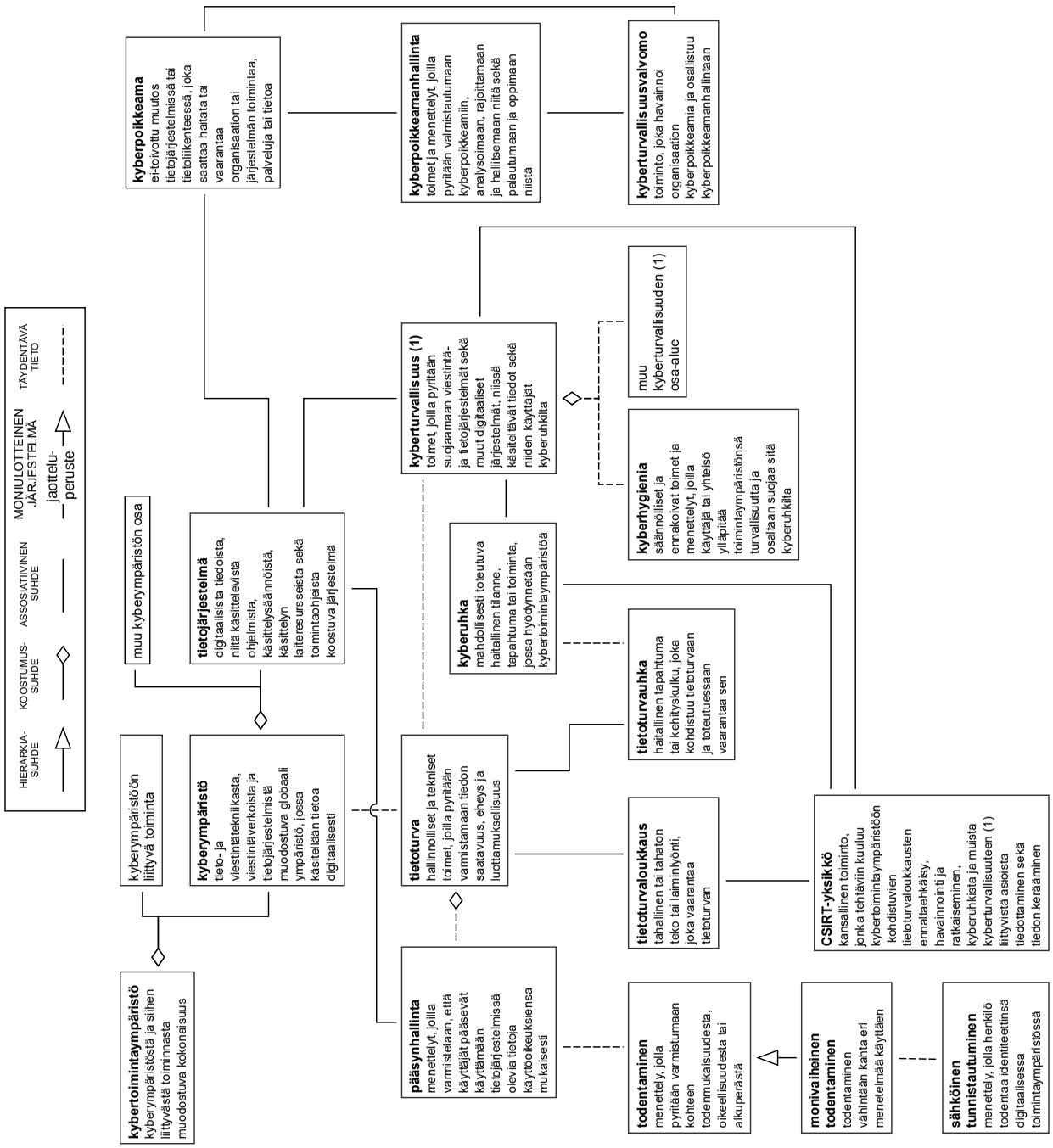
huomautus

Tunnistautumisen menetelmät ja tunnistusvälineet perustuvat siihen, mitä henkilö tietää (esimerkiksi PIN-koodi), mitä henkilöllä on hallussaan (esimerkiksi mobiilisovellus) tai kuka henkilö on (sormenjälki tai muu käyttäjän yksilöivä ominaisuus).

Vahva sähköinen tunnistautuminen tarkoittaa tunnistautumista kahta tai useampaa menetelmää käyttäen, vrt. *monivaiheinen todentaminen*.

Englanninkielinen termi identification viittaa tunnistautumisen lisäksi myös tunnistamiseen ja tunnistukseen.

Käsitejärjestelmäkaavio: Kyberturvallisuus ja tietoturva



Käsitejärjestelmäkaavio 1. *Kyberturvallisuus ja tietoturva.*

2 Kyberhyökkäys

17

kyberhyökkäys

sv cyberattack; cyberangrepp *n*

en cyberattack; cyber attack; cyberspace attack <Nato>

määritelmä

kyberympäristössä tai sen kautta tapahtuva toiminta, jolla pyritään kohteen vahingoittamiseen, lamauttamiseen tai oikeudettomaan käyttöön

huomautus

Erityyppisiä kyberhyökkäyksiä ovat esimerkiksi *palvelunestohyökkäykset*, *toimitusketjuhyökkäykset*, *tietojenkalastelu*, *tietomurto* ja *kohdistetut kyberhyökkäykset*.

Kyberhyökkäyksen tavoite voi vaihdella henkilökohtaisesta edusta esimerkiksi taloudellisiin, ideologisiin tai poliittisiin tavoitteisiin. Joissakin tapauksissa vakavan kyberhyökkäyksen voidaan katsoa ylittävän aseellisen konfliktin kynnyksen.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaaviot: Kyberhyökkäys ja Kyberuhkat

18

palvelunestohyökkäys

sv överbelastningsattack; överbelastningsangrepp *n*; tillgänglighetsattack

en denial of service attack; DoS attack; denial of service

määritelmä

kyberhyökkäys, jolla pyritään kuormittamaan ja siten lamaannuttamaan jokin palvelu tai *tietojärjestelmä* ja sillä tavoin estämään tietty toiminta tai palvelu

huomautus

Palvelunestohyökkäys voi esimerkiksi lamaannuttaa verkkosivuston tai -palvelun liian suurella määrällä palvelupyyntöjä.

Käsitejärjestelmäkaavio: Kyberhyökkäys

19

toimitusketjuhyökkäys

ei: tietovuoto

sv leverantörsattack; leveranskedjeattack

en supply chain attack

määritelmä

kyberhyökkäys, jossa organisaation *tietojärjestelmiin* murtaudutaan sen käyttämien verkostojen, palveluiden, tuotteiden tai avoimen lähdekoodin projektien kautta

huomautus

Toimitusketjuhyökkäyksen tavoitteena on jalansijan saavuttaminen eri organisaatioissa toimitusketjun varrella. Kun jalansija on varmistettu, voidaan sitä käyttää erilaisiin jatkohyökkäyksiin, kuten *tietomurtoihin* ja kiristyshaittaohjelmahyökkäyksiin.

Toimitusketjuhyökkäyksen reittinä voivat olla organisaation yhteistyökumppanit tai sen käyttämät palveluntarjoajat, ohjelmistot tai laitteet. Hyökkääjä voi esimerkiksi tunkeutua toimittajan järjestelmiin ja saastuttaa toimitusketjussa käytetyn osan omalla haittakoodillaan, jonka jälkeen haittakoodi leviää normaalia tuotteen jakelukanavaa pitkin yhteistyö- ja asiakasorganisaatioihin.

Käsitejärjestelmäkaavio: Kyberhyökkäys

20

tietojenkalastelu; tietojenkalasteluhyökkäys

sv nätfiske *n*; nätfiskeattack; phishing

en phishing

määritelmä

kyberhyökkäys, jonka tavoitteena on hankkia arkaluontoista tietoa tekeytymällä tiedon käyttöön oikeutetuksi ja käyttämällä hyväksi tiedon käyttöön oikeutettuja henkilöitä

huomautus

Tietojenkalastelu voi kohdistua yhteen tai useampaan henkilöön. Usein tietojenkalastelulla pyritään manipuloimaan käyttäjää esimerkiksi luovuttamaan käyttäjätietonsa.

Käsitejärjestelmäkaavio: Kyberhyökkäys

21
kohdistettu kyberhyökkäys; kohdistettu hyökkäys; > kohdistettu haittaohjelmahyökkäys

sv riktad cyberattack; målinriktad cyberattack; > riktat sabotageprogram *n*

en advanced persistent threat; APT; advanced persistent threat attack; APT attack
rather than: < targeted attack; > targeted malware attack

määritelmä
tavoitehakuinen ja usein *kehittyneen kyberuhkatoimijan* toteuttama pitkäkestoinen *kyberhyökkäys*, joka kohdistuu tiettyyn rajattuun kohteeseen

huomautus
Kohdistettu kyberhyökkäys voi suuntautua esimerkiksi yritykseen, toimialaan, valtionhallinnon organisaatioon tai rajattuun joukkoon henkilöitä. Tavoitteena on usein kohteen kriittisen tiedon haltuun saaminen tai kohteen toiminnan muuttaminen.

Kohdistettu kyberhyökkäys voi olla *kyberoperaatio* tai osa kyberoperaatiota.

Käsitejärjestelmäkaavio: Kyberhyökkäys

22
tietomurto

sv dataintrång *n*

en intrusion; unlawful access to an information system <rikosnimike rikoslaissa>
rather than: computer intrusion; computer break-in
not: data breach; breach

määritelmä
kyberhyökkäys, jossa tunkeudutaan luvatta *tietojärjestelmään* tai päästään oikeudettomasti käsiksi tietojärjestelmässä olevaan tietoon

huomautus
Tietomurrosta voi seurata esimerkiksi tietovuoto, henkilötietojen *tietoturvaloukkaus* tai *kiristyshaittaohjelman* ujuttaminen tietojärjestelmään. Tietomurron seuraukset eivät välttämättä ole välittömiä, vaan *kyberuhkatoimija* voi pyrkiä hyödyntämään saamiaan tietoja tai pääsyä tietojärjestelmään myöhemmin.

Tietomurrossa kyberhyökkäyksen toteuttaja voi saada käsiinsä henkilötietoja, laskutustietoja, tilitietoja, maksukortteja, yrityssalaisuuksia, arkaluonteisia tietoja asiakkaista tai yksittäisistä työntekijöistä tai muuta salassa pidettävää tai rahan arvoista tietoa.

Englanninkieliset termit data breach ja breach viittaavat käsitteeseen tietoturvaloukkaus, jossa tietoja vaarantuu tai väärinkäytetään.

Käsitejärjestelmäkaavio: Kyberhyökkäys

23
haavoittuvuus

sv sårbarhet

en vulnerability

määritelmä
heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamiseen *kyberympäristössä*

huomautus
Haavoittuvuudet ovat tyypillisesti virheitä, jotka ovat jääneet *tietojärjestelmiin* kehityksen aikana. Haavoittuvuuksia voi olla esimerkiksi *tietojärjestelmissä*, sovelluksissa tai laitteissa tai niitä voi aiheutua ihmisten toiminnan seurauksena, esimerkiksi puutteellisen *kyberhygienian* takia.

Haavoittuvuuksia on erilaisia ja eritasoisia.

Nollapäivähaavoittuvuus on tietojärjestelmässä oleva haavoittuvuus, jolle on hyväksikäyttömenetelmä ja johon ei ole sen havaitsemishetkellä saatavilla korjausta.

Käsitejärjestelmäkaavio: Kyberhyökkäys

24
hyökkäyspinta-ala; hyökkäyspinta
sv attackyta; angreppsyta
en attack surface

määritelmä
fyysiset, virtuaaliset ja kognitiiviset rajapinnat, joita mahdollinen hyökkääjä voi hyödyntää *kyberhyökkäyksen* tekemiseen

huomautus
Fyysinen rajapinta on esimerkiksi kahden laitteen liitoskohta kuten kaapeli tai liitin, kun taas virtuaalinen rajapinta tarkoittaa esimerkiksi sovellusten tai palveluiden välisiä virtuaalisia yhtymäkohtia. Kognitiivisella rajapinnalla puolestaan tarkoitetaan ihmisen ja teknologian välistä vuorovaikutusta.

Kyberhyökkäyksiä tekemään pyrkivät toimijat kartoittavat jatkuvasti mahdollisia hyökkäyspinta-aloja. Hyökkäyspinta-alaa lisäävät muun muassa internetiin avoimet tietoliikenneportit, suojaamattomat *tietojärjestelmät* ja verkkopalveluissa olevat *haavoittuvuudet*. Kyberhyökkäyksiltä suojautumiseksi hyökkäyspinta-ala pyritään pitämään mahdollisimman pienenä.

Yhteiskunnan digitalisoituminen ja esimerkiksi esineiden internetin (Internet of Things, IoT) yleistyminen kasvattavat hyökkäyspinta-alaa, mikä lisää *kyberuhkien* toteutumisen mahdollisuutta.

Käsitejärjestelmäkaaviot: Kyberhyökkäys ja Kyberuhkat

25
haittaohjelma; ~ haittakoodi
sv skadligt program *n*; skadlig programvara; skadeprogram *n*; sabotageprogram *n*; ~ skadlig kod
en malware; malicious software; ~ malicious code; ~ malicious logic

määritelmä
ohjelma, jonka toiminta aiheuttaa tarkoituksellisesti *tietojärjestelmän* tai laitteen käyttäjän kannalta ei-toivottuja tapahtumia tietoverkossa, tietojärjestelmässä tai sen osassa

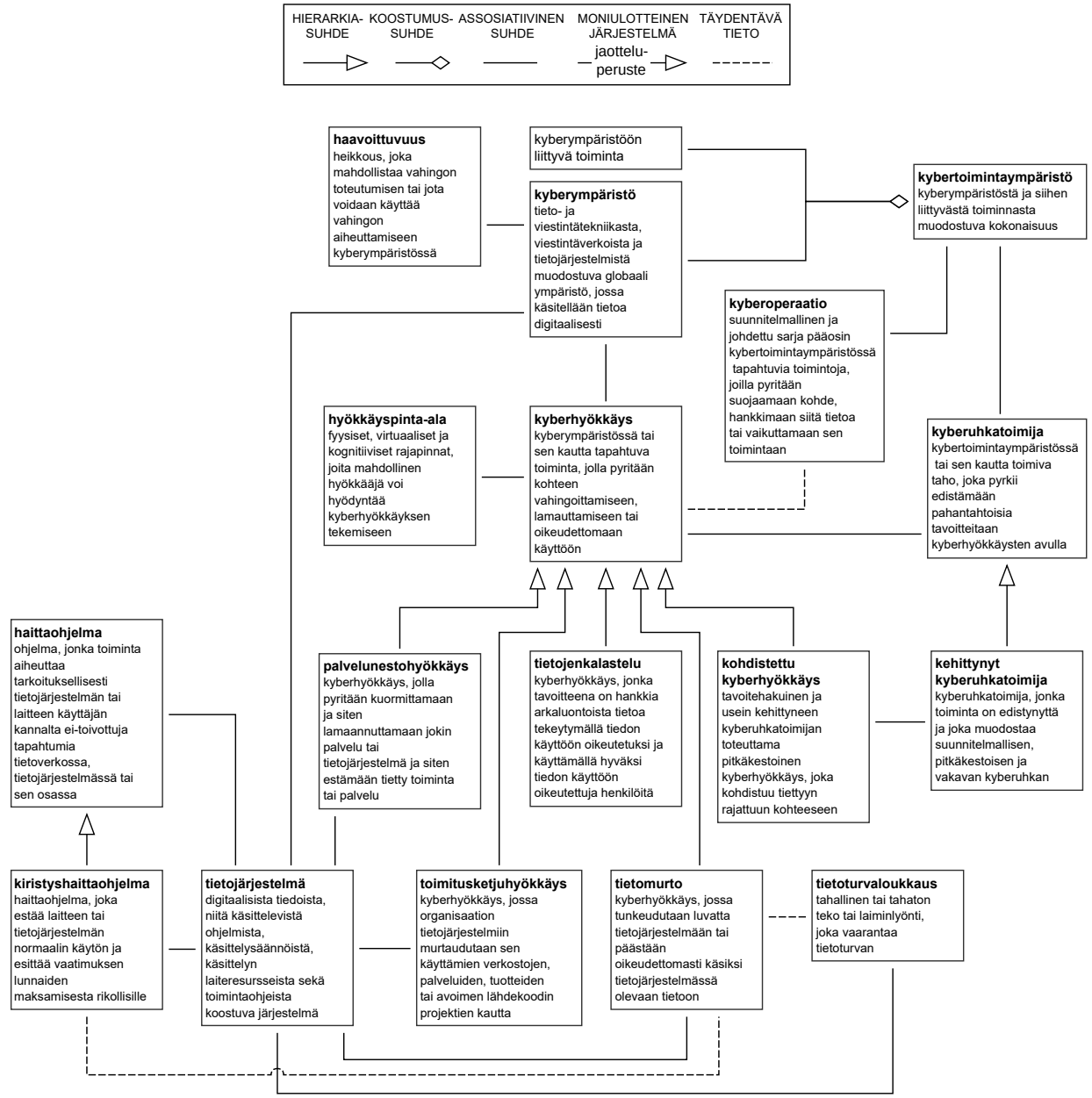
Käsitejärjestelmäkaavio: Kyberhyökkäys

26
kiristyshaittaohjelma; kiristysohjelma
sv utpressningsprogram *n*; gisslanprogram *n*
en ransomware

määritelmä
haittaohjelma, joka estää laitteen tai *tietojärjestelmän* normaalin käytön ja esittää vaatimuksen lunnaiden maksamisesta rikollisille

huomautus
Kiristyshaittaohjelma voi kohdistua yksittäiseen käyttäjään tai kokonaiseen organisaatioon.

Käsitejärjestelmäkaavio: Kyberhyökkäys



Käsitejärjestelmäkaavio 2. *Kyberhyökkäys.*

3 Kyberuhkat

27

kyberuhka

sv cyberhot *n*; cybersäkerhetshot *n*; hot *n* mot cybersäkerheten

en cyber threat; cyberthreat; cybersecurity threat; cyber security threat

määritelmä

mahdollisesti toteutuva haitallinen tilanne, tapahtuma tai toiminta, jossa hyödynnetään *kybertoimintaympäristöä*

huomautus

Vakavat kyberuhkat voivat aiheutua digitaalisessa viestintäympäristössä toteutettavista, yhteiskunnan turvallisuutta vaarantavista teoista. Tällaisista teoista aiheutuvia kyberuhkia ovat esimerkiksi *kyberrikollisuus* ja *kybervakoilu*.

Vakavat kyberuhkat voivat kohdistua *yhteiskunnan elintärkeitä toimintoja*, kansallista *kriittistä infrastruktuuria* tai kansalaisia vastaan joko suoraan tai välillisesti. Ne voivat olla peräisin maan rajojen sisältä tai niiden ulkopuolelta.

Suomi suojautuu vakavilta kyberuhkilta *kansallisen kyberpuolustuksen*, *kyberturvallisuuden (1)* ja *kyberdiplomatian* keinoin.

Tiettyyn toimijaan liittyvää kyberuhkaa arvioidaan toimijan kyvyn ja tahdon kautta (kyky x tahto).

Kyberuhkan voivat muodostaa esimerkiksi erilaiset *haavoittuvuudet* yhdessä *hyökkäyspinta-alan* kanssa.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaaviot: Kyberturvallisuus ja tietoturva, Kyberuhkat ja Kybertoimintaympäristö ja siihen liittyvä toiminta

28

kyberrikollisuus; ~ tietoverkkorikollisuus

sv cyberbrottslighet; cyberkriminalitet; ~ nätbrottslighet

en cybercrime; cyber crime

määritelmä

rikollisuus, joka muodostuu viestintäverkkoja ja *tietojärjestelmiä* hyödyntäen tehdyistä sekä niihin kohdistuvista rikoksista

huomautus

Kyberrikollisuuden tavoitteena voi olla esimerkiksi taloudellinen tai poliittinen hyöty, tiedon varastaminen, palveluiden häiritseminen tai identiteettivarkaudet.

Kyberrikollisuuden vaikutukset voivat kohdistua niin valtioihin, yksittäisiin kansalaisiin kuin organisaatioiden toimintaan.

Kyberrikollisuus ylittää usein kansalliset rajat, koska viestintäverkoissa ei ole samanlaisia fyysisiä rajoitteita kuin monilla perinteisillä rikoksilla.

Vakava kyberrikollisuus voi vaarantaa *yhteiskunnan elintärkeät toiminnot*, uhata kansallista turvallisuutta tai aiheuttaa muuten yhteiskuntaan laajasti vaikuttavia häiriöitä.

Kyberrikolliset ovat *kyberuhkatoimijoita*.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kyberuhkat

29

kybervakoilu; tietoverkkovakoilu

sv cyberspionage *n*; cyberspionerі *n*; ~ nätspionage *n*; ~ nätspionerі *n*

en cyber espionage; cyber spying

määritelmä

vakoilu, jossa hyödynnetään *kybertoimintaympäristöä*

huomautus

Kybervakoilu voi kohdistua valtioihin, yrityksiin tai muihin organisaatioihin tai yksilöihin.

Kybervakoilussa voidaan käyttää hyväksi esimerkiksi *kohdistettuja kyberhyökkäyksiä*.

Kybervakoilu on kansallisen lainsäädännön mukaan pääsääntöisesti lainvastaista toimintaa (vrt. *tietoverkkotiedustelu*).

Käsitejärjestelmäkaavio: Kyberuhkat

30
kyberuhkatoimija; < uhkatoimija
sv cyberhotaktör; < hotaktör; < fientlig aktör
en cyber threat actor; cyberthreat actor; < threat actor

määritelmä
kybertoimintaympäristössä tai sen kautta toimiva taho, joka pyrkii edistämään pahantahtoisia tavoitteitaan *kyberhyökkäysten* avulla

huomautus
Kyberuhkatoimija voi olla esimerkiksi yksittäinen henkilö, ryhmä, organisaatio tai valtiollinen toimija. Toiminnan tavoite voi vaihdella henkilökohtaisesta edusta esimerkiksi taloudellisiin, ideologisiin tai poliittisiin tavoitteisiin.

Kyberuhkatoimijan toiminta muodostaa *kyberuhkan*.

Ruotsin ja englannin kielissä on tavallisempaa käyttää lyhyempää termiä ilman cyber-alkua silloin, kun yhteys kybertoimintaympäristöön on muutoin termin käyttöyhteydessä selvä.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaaviot: Kyberhyökkäys, Kyberuhkat ja Kybertoimintaympäristö ja siihen liittyvä toiminta

31
kehittynyt kyberuhkatoimija (uudistermi)**; APT-toimija**
sv kvalificerad cyberhotaktör; APT-aktör
en advanced persistent threat actor; APT actor

määritelmä
kyberuhkatoimija, jonka toiminta on edistynyttä ja joka muodostaa suunnitelmallisen, pitkäkestoisen ja vakavan *kyberuhkan*

huomautus
Kehittyneelle kyberuhkatoimijalle on tyypillistä vakiintuneet toimintatavat ja tekniikat, järjestäytyneisyys sekä merkittävät kyvyt ja resurssit toteuttaa *kyberhyökkäyksiä*.

Kehittyneitä kyberuhkatoimijoita voidaan määritellä ja nimetä eri tavoin erilaisissa yhteyksissä.

APT-lyhenne tulee englannin kielen sanoista advanced persistent threat, joilla viitataan kehittyneen kyberuhkatoimijan toiminnan erityiseen vaikuttavuuteen ja pitkäkestoisuuteen.

Käsitejärjestelmäkaaviot: Kyberhyökkäys ja Kyberuhkat

32
<kyberturvallisuus>
sijaistoimija
mieluummin kuin: proxy-toimija
sv proxyaktör
en cyber proxy; < proxy

määritelmä
kyberuhkatoimija, joka toimii toisen osapuolen lukuun peittääkseen *kyberhyökkäyksen* todellisen alkuperän

huomautus
Sijaistoimija voi olla esimerkiksi yritys, pahantahtoinen kyberaktivisti tai rikollisryhmä, jota valtiollinen toimija hyödyntää.

Valtiollinen kyberuhkatoimija voi käyttää sijaistoimijana esimerkiksi julkisen ja tutkimussektorin toimijoita muun muassa asettamalla näille erilaisia velvoitteita tai käyttämällä näitä esimerkiksi tiedonhankintaan, *kyberoperaatioihin* tai ns. jalansijojen hankkimiseen.

Käsitejärjestelmäkaavio: Kyberuhkat

33

kyberuhkatoiminnan myötävaikuttaja (uudistermi)

mieluummin kuin: TAE-toimija

sv möjliggörare för hotaktivitet; < möjliggörare

en threat activity enabler; < enabler

määritelmä

taho, jota *kyberuhkatoimijat* voivat hyödyntää *kyberhyökkäysten* toteuttamiseen

huomautus

Kyberuhkatoiminnan myötävaikuttajat voivat olla hyvin erilaisia riippuen siitä, millainen kyberuhkatoimija on kyseessä. Kyberuhkatoiminnan myötävaikuttaja voi olla esimerkiksi yritys, kuten palveluntarjoaja tai verkonvälittäjä, jonka infrastruktuuria kyberuhkatoimija voi käyttää.

Käsitejärjestelmäkaavio: Kyberuhkat

34

kyberuhkamallinnus; < uhkamallinnus

sv cyberhotmodellering; < hotmodellering

en cyber threat modelling; cyberthreat modelling; < threat modelling

määritelmä

toiminta, jonka avulla kartoitetaan *tietojärjestelmän* tai ohjelmiston *hyökkäyspinta-alat* ja hyökkäyspolut sekä mallinnetaan tietojärjestelmään tai niitä hyödyntäviin toimintaprosesseihin kohdistuvat uhkat

huomautus

Kyberuhkamallinnusta voidaan käyttää ennakoinnin työkaluna *kyberturvallisuuteen (1)* liittyvien uhkien hallinnassa.

Ruotsin ja englannin kielissä on tavallisempaa käyttää lyhyempää termiä ilman cyber-alkua silloin, kun yhteys *kybertoimintaympäristöön* on muutoin termin käyttöyhteydessä selvä.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kyberuhkat

35

kyberuhkanmetsästys; kyberuhkien metsästys; < uhkanmetsästys

sv cyberhotjakt; < hotjakt

en cyber threat hunting; cyberthreat hunting; < threat hunting

määritelmä

proaktiivinen toiminta niiden *kyberuhkien* löytämiseksi, jotka ovat läpäisseet tietoturvakontrollit

huomautus

Kyberuhkanmetsästyksen tavoitteena on havaita aktiiviset tai vielä havaitsemattomat tunkeutumiset tietoverkkoihin, järjestelmiin tai päätelaitteisiin varhaisessa vaiheessa ennen kuin ne kärjistyvät vakaviksi vaaratilanteiksi.

Ruotsin ja englannin kielissä on tavallisempaa käyttää lyhyempää termiä ilman cyber-alkua silloin, kun yhteys *kybertoimintaympäristöön* on muutoin termin käyttöyhteydessä selvä.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kyberuhkat

36
kyberuhkatieto; < uhkatieto

sv cyberhotinformation; < hotinformation

en cyber threat intelligence (1); cyberthreat intelligence (1); < threat intelligence (1)

määritelmä
tieto, jonka avulla saadaan käsitys menneistä, nykyisistä ja mahdollisista tulevista *kyberuhkista* ja jota käytetään organisaation päätöksenteon tukena *tietoturvan* ja *kyberturvallisuuden (1)* parantamiseksi

huomautus
Kyberuhkatietoa ovat esimerkiksi uhkatunnisteet eli IoC-tiedot (indicators of compromise), *kyberuhkatoimijoiden* profiilit, tiedot näiden suorittamista operaatioista sekä haavoittuvuustiedot.

Kyberuhkatieto voi olla teknis-taktista (kuten IP-osoitteet tai *haittaohjelmien* tunnisteet), operatiivista (kuten tietoa *kyberhyökkäyksen* ajoituksesta tai menetelmistä) tai strategista (kuten johdon päätöksentekoa tukeva kattavampi analyysi).

Kyberuhkatietoa voidaan käyttää esimerkiksi kyberuhkien tunnistamiseen ja torjumiseen, attribuointiin, *haavoittuvuuksien* arviointiin, tietoturvapolitiikan ja -strategian kehittämiseen tai organisaation reagointikyvyn parantamiseen kuten *kyberpoikkeamanhallintaan*.

Kyberuhkatiedon jakamisella eri toimijoiden kesken voidaan parantaa yhteiskunnan *kyberresilienssiä*.

Ruotsin ja englannin kielissä on tavallisempaa käyttää lyhyempää termiä ilman cyber-alkua silloin, kun yhteys *kybertoimintaympäristöön* on muutoin termin käyttöyhteydessä selvä.

Englanninkielinen termi (cyber) threat intelligence voi viitata myös *kyberuhkatiedusteluun*. Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kyberuhkat

37
kyberuhkatiedustelu; < uhkatiedustelu

sv underrättelser *pl* om cyberhot; underrättelseinhämtning om cyberhot; < hotunderrättelser *pl*

en cyber threat intelligence (2); cyberthreat intelligence (2); < threat intelligence (2)

määritelmä
kyberuhkatiedon kerääminen, analysointi ja jakaminen muiden toimijoiden kanssa

huomautus
Kyberuhkatiedustelu ei ole pelkästään turvallisuus- ja tiedusteluviranomaisten toimintaa, vaan sitä voivat tehdä useat eri viranomaiset tai yksityiset organisaatiot. Kyberuhkatiedustelu voi olla esimerkiksi *kyberturvallisuusvalvomon* tehtävä.

Kyberuhkatiedustelulla voidaan saada tietoa myös *kyberuhkatoimijoista*.

Kyberuhkatiedustelu on yksi *kybertiedustelun* osa-alueista.

Englanninkielinen termi (cyber) threat intelligence viittaa usein tiedustelutoiminnan sijasta uhkia koskevaan tietoon, kyberuhkatietoon. Ruotsin ja englannin kielissä on tavallisempaa käyttää lyhyempää termiä ilman cyber-alkua silloin, kun yhteys *kybertoimintaympäristöön* on muutoin termin käyttöyhteydessä selvä. Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaaviot: Kyberuhkat ja Kybertoimintaympäristö ja siihen liittyvä toiminta

38

murrosteknologia; murroksellinen teknologia; ~ kehittyvä teknologia

sv omvälvande teknologi; disruptiv teknologi; ~ framväxande teknologi

en disruptive technology; ~ emerging technology; ~ emerging and disruptive technology; ~ EDT

määritelmä

teknologia, jolla on edellytyksiä aiheuttaa merkittäviä muutoksia yhteiskunnassa tai toimintatavoissa

huomautus

Murrosteknologioita ovat esimerkiksi tekoäly, kvanttiteknologia ja uuden sukupolven viestintäverkot.

Murrosteknologioihin liittyy mahdollisuuksia parantaa yhteiskunnan tuottavuutta, tehokkuutta ja kilpailukykyä. Erilaisten murrosteknologioiden yhteisvaikutuksia on kuitenkin hyvin vaikea ennakoida, ja siksi murrosteknologioihin liittyviä riskejä voi olla vaikea ennustaa ja hallita. Lisäksi murrosteknologiat tuovat mukanaan uusia ja osin vielä tuntemattomia *kyberuhkia* muun muassa avaamalla uusia *hyökkäyspinta-aloja*.

Murrosteknologiat voivat aiheuttaa esimerkiksi merkittäviä taloudellisia tai geopoliittisia muutoksia.

Murrosteknologiat ovat usein luonteeltaan strategisia kaksoiskäyttöteknologioita eli ne soveltuvat sekä siviili- että sotilaskäyttöön.

Käsitejärjestelmäkaavio: Kyberuhkat

39

ISAC-tiedonvaihtoryhmä

sv ISAC-informationsutbytesgrupp; ISAC-grupp

en information sharing and analysis centre, ISAC
rather than: ISAC information sharing group; ISAC group

määritelmä

vapaaehtoisuuteen ja luottamukseen perustuva yhteistyö- ja tiedonvaihtoverkosto, jonka tarkoitus on parantaa organisaatioiden kykyä suojautua *kyberuhkilta*

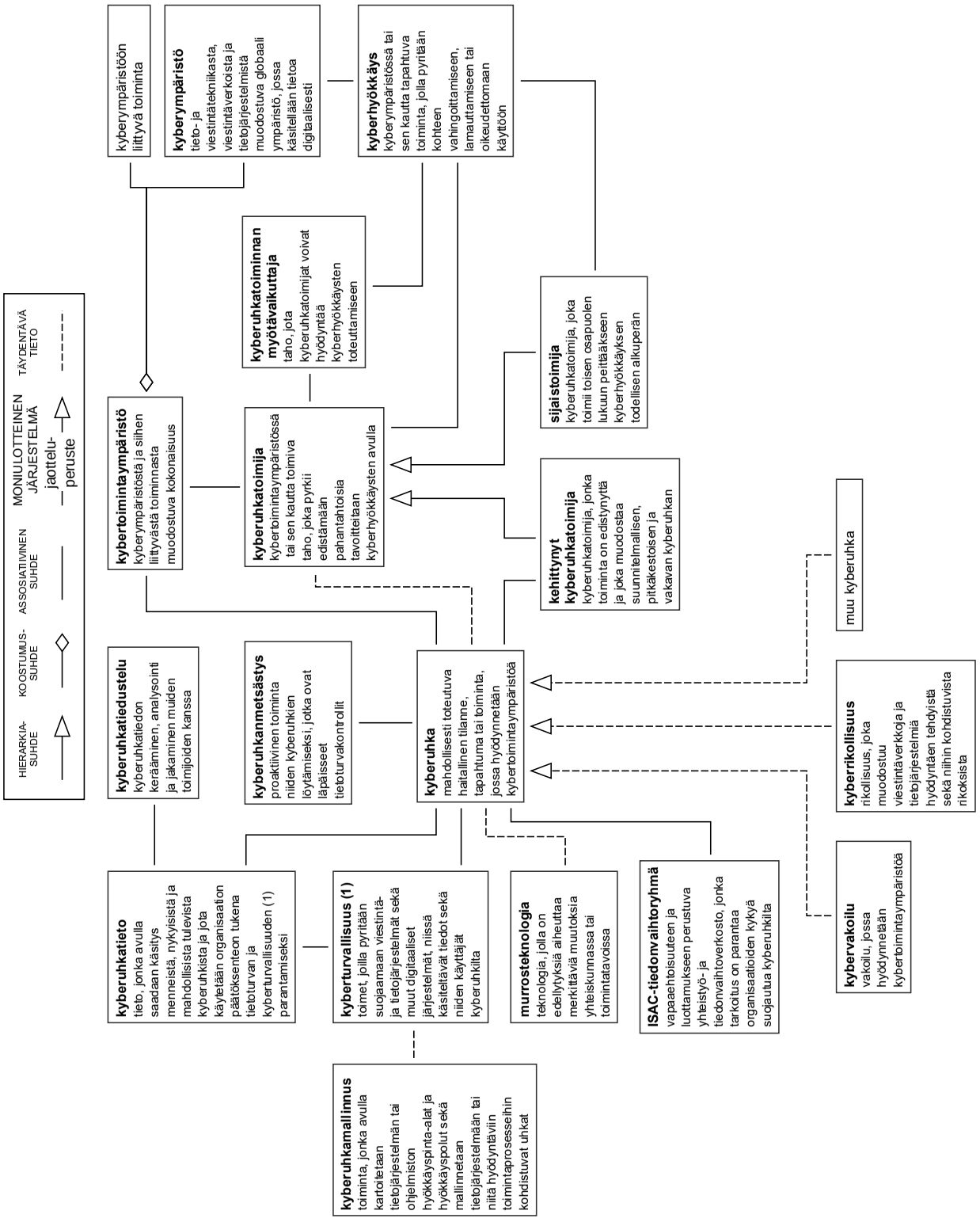
huomautus

Suomessa useimpien ISAC-tiedonvaihtoryhmien koordinointitehtävä on säädetty kyberturvallisuuslaissa (124/2025) Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen *CSIRT-yksikölle*.

ISAC-tiedonvaihtoryhmiä on perustettu kansainvälisesti useille eri toimialoille ja ne tuovat yhteen julkisen ja yksityisen sektorin toimijoita.

ISAC-lyhenne tulee englannin kielen sanoista information sharing and analysis centre.

Käsitejärjestelmäkaavio: Kyberuhkat



Käsitejärjestelmäkaavio 3. *Kyberuhkat.*

4 Kybertoimintaympäristö ja siinä tapahtuva toiminta

40

kybertoimintaympäristö

mieluummin kuin: kyberympäristö

sv cybermiljö (1); cyberdomän

en cyber environment; cyber domain
not: cyber operating environment

määritelmä

kyberympäristöstä ja siihen liittyvästä toiminnasta muodostuva kokonaisuus

huomautus

Kybertoimintaympäristö painottaa kyberympäristön hyödyntämistä tavoitteellisen toiminnan näkökulmasta.

Esimerkkejä kybertoimintaympäristöistä ovat *tietojärjestelmiin* perustuvat ydinvoimalan ohjausjärjestelmä, elintarvikkeiden kuljetus- ja logistiikkajärjestelmä, liikenteen ohjausjärjestelmät ja pankki- ja maksujärjestelmät, järjestelmien käyttäjät sekä niihin liittyvät prosessit ja käytännöt.

Termien kybertoimintaympäristö ja kyberympäristö käyttö vaihtelee. Tässä sanastossa termeillä viitataan kahteen eri käsitteeseen, mutta toisissa yhteyksissä nämä käsitteet ymmärretään osin päällekkäisinä. Kyberympäristö ja kybertoimintaympäristö voivat joissakin tapauksissa viitata myös samaan käsitteeseen.

Myös ruotsin ja englannin kielissä käsitteet voidaan ymmärtää osin päällekkäisinä ja vastineiden käyttö vaihtelee. Ruotsinkielisen termin cyberdomän ja englanninkielisen termin cyber domain käyttöyhteys on usein sotilaallinen.

Joissakin yhteyksissä kybertoimintaympäristöstä käytetään myös termiä kyberavaruus, mutta tässä sanastossa sitä ei suositeta kybertoimintaympäristön synonyymiksi.

Käsitejärjestelmäkaaviot: Kyberturvallisuus ja tietoturva, Kyberhyökkäys, Kyberuhkat ja Kybertoimintaympäristö ja siihen liittyvä toiminta

41

kyberturvallisuuden tilannekuva; kybertilannekuva

sv lägesbild över cybersäkerheten; cyberlägesbild; < situationsmedvetenhet när det gäller cybersäkerhet

en cybersecurity situational picture; cybersecurity situation picture; < cybersecurity situational awareness; < cybersecurity situation awareness

määritelmä

koottu kuvaus tietyllä hetkellä vallitsevasta käytettävyys- ja turvallisuustilanteesta *kybertoimintaympäristössä*

huomautus

Kyberturvallisuuden tilannekuva muodostetaan kunkin organisaation tarpeisiin sopivasta näkökulmasta ja usein yhteistyössä eri toimijoiden kesken. Se tukee tilanneymmärryksen muodostumista sekä organisaation päätöksentekoa ja toimintaa.

Kyberturvallisuuden tilannekuva perustuu havaintoihin, tiedonvaihtoon, mittareihin, arviointeihin ja analyyseihin.

Kyberturvallisuuden tilannekuvaa voidaan tarkastella taktisella, operatiivisella tai strategisella tasolla.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksella on lakisääteinen tehtävä koota ja koordinoida kansallista kyberturvallisuuden tilannekuvaa. Tietoja kerätään *kyberekosysteemissä* ja tilannekuvaa tuotetaan eri kohderyhmille yksittäisistä palveluiden käyttäjistä valtiojohtoon.

Ks. myös käsite tilannetietoisuus Kokonaisturvallisuuden sanastossa (TSK 50, 2017).

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*. Cybersecurity voidaan kirjoittaa myös erikseen (cyber security).

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

42
kyberekosysteemi; ~ kyberturvallisuuden ekosysteemi
sv cyberekosystem *n*; ~ ekosystem *n* för cybersäkerhet
en cyber ecosystem; ~ cybersecurity ecosystem; ~ cyber security ecosystem

määritelmä
kybertoimintaympäristössä toimiva, keskenään vuorovaikutuksessa olevien tutkimuksen, julkishallinnon ja kolmannen sektorin toimijoiden, yritysten ja yksilöiden välinen verkosto

huomautus
Termillä kyberturvallisuuden ekosysteemi viitataan käsitteeseen, jossa korostuu tavoite parantaa digitaalisen yhteiskunnan kestävyyttä ja sietokykyä kybertoimintaympäristön haitallisia ilmiöitä vastaan.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

43
kyberresilienssi; ~ kybersietoisuus
sv cyberresiliens
en cyber resilience; cyberresilience

määritelmä
yhteiskunnan, organisaation, yhteisön tai yksilön kyky ylläpitää toimintakykyään *kybertoimintaympäristössä* ja sen muuttuvissa olosuhteissa sekä valmius kohdata siinä ilmeneviä häiriöitä ja uhkia, palautua niistä ja tarvittaessa reagoida niihin

huomautus
Kyberresilienssiä voidaan vahvistaa esimerkiksi hyvällä *kyberhygienialla*.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

44
jatkuvuudenhallinta
sv kontinuitetshantering; hantering av kontinuiteten
en continuity management; > business continuity management

määritelmä
organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan suunnitelma ja toimintatapa vakavien häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa

huomautus
Jatkuvuudenhallinta on osa kokonaisvaltaista riskienhallintaa. *Kyberturvallisuuden (1)* ja *kyberresilienssin* yhteydessä jatkuvuudenhallinnalla varmistetaan, että organisaatio pystyy jatkamaan toimintaansa myös vakavien *kyberpoikkeamien* tai *kyberhyökkäysten* aikana sekä palautumaan niistä.

Jatkuvuudenhallinta on organisaation ylimmän johdon hyväksymää suunnitelmallista strategista ja operatiivista toimintaa, jolla organisaatio varautuu hallitsemaan häiriötilanteet ja jatkamaan toimintaa ennalta määritellyllä hyväksyttävällä tasolla.

Jatkuvuudenhallinta on yleensä omaehtoista toimintaa, mutta joillakin aloilla organisaatiot ovat myös lailla velvoitettuja varmistamaan toimintansa eri olosuhteissa.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

45
kansallinen kyberturvallisuus; kyberturvallisuus (2)
sv nationell cybersäkerhet
en national cybersecurity; national cyber security

määritelmä
toimet, joiden avulla varaudutaan, tunnistetaan, torjutaan ja siedetään *kybertoimintaympäristön* häiriöitä ja niiden vaikutuksia *yhteiskunnan elintärkeisiin toimintoihin* ja palveluihin, toivutaan niistä sekä varmistetaan osaltaan kokonaisturvallisuuden toimintaedellytykset

huomautus
Kansallisen kyberturvallisuuden toimiin osallistuvat julkinen hallinto, yritykset ja yhteisöt sekä kansalaisyhteiskunta.

Kokonaisturvallisuuden näkökulmasta kansallinen kyberturvallisuus on kokonaisturvallisuuden toteuttamista kybertoimintaympäristössä. Tähän sisältyvät muun muassa kansallinen turvallisuus, maanpuolustus ja huoltovarmuus.

Kansallisesta kyberturvallisuudesta käytetään joissakin yhteyksissä (esimerkiksi Yhteiskunnan turvallisuusstrategia (Valtioneuvoston julkaisuja 2025:1)) myös termiä kyberturvallisuus (2).

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

46
yhteiskunnan elintärkeä toiminto
sv kritiska samhällsfunktioner *pl*; vitala samhällsfunktioner *pl*; samhällets vitala funktioner *pl*
en functions *pl* vital to society; vital functions *pl* of society

määritelmä
toiminto, joka on välttämätön yhteiskunnan toimivuuden kannalta

huomautus
Yhteiskunnan elintärkeitä toimintoja ovat johtaminen, kansainvälinen ja EU-toiminta, puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri ja huoltovarmuus, väestön toimintakyky ja palvelut sekä henkinen kriisinkestävyys. Nämä toiminnot on kuvattu Yhteiskunnan turvallisuusstrategiassa (Valtioneuvoston julkaisuja 2025:1).

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

47
kriittinen infrastruktuuri
sv kritisk infrastruktur
en critical infrastructure

määritelmä
hyödykkeet, tilat, laitteistot, verkostot, järjestelmät, näiden osat ja tärkeät palvelut, jotka ovat välttämättömiä *yhteiskunnan elintärkeiden toimintojen* ylläpitämiseksi tai muiden keskeisten palvelujen tarjoamiseksi

huomautus
Kriittiseen infrastruktuuriin kuuluvat muun muassa energian tuotanto-, siirto- ja jakelujärjestelmät, liikenne ja logistiikka, tieto- ja viestintäjärjestelmät sekä vesi- ja jätehuolto.

Kriittisestä infrastruktuurista kirjataan laissa yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (310/2025) sekä valtioneuvoston päätöksessä huoltovarmuuden tavoitteista (568/2024).

Kriittisen infrastruktuurin yhteydessä käytetään usein englanninkielisiä ilmauksia critical infrastructure protection (CIP), joka tarkoittaa kriittisen infrastruktuurin suojaamista, ja critical information infrastructure protection (CIIP), joka tarkoittaa kriittisen tietoinfrastruktuurin suojaamista.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

48
puolustuskyvylle kriittinen infrastruktuuri
sv infrastruktur som är kritisk för försvarsförmågan; kritisk infrastruktur för försvarsförmågan
en infrastructure critical for defence capability; > mission vital infrastructure; > mission critical infrastructure

määritelmä
puolustusjärjestelmän ja *kriittisen infrastruktuurin* rakenteet, palvelut ja niihin liittyvät toiminnot sekä ne *yhteiskunnan elintärkeät toiminnot*, jotka ovat välttämättömiä maanpuolustuksen toimintaedellytyksille kaikissa valmiustiloissa

huomautus
Puolustuskyky koostuu siviili- ja sotilaskyvykkyyksistä.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

49
<Suomi>
kansallinen kyberpuolustus
sv nationellt cyberförsvar *n*
en national cyber defence; national cyberdefence

määritelmä
kansalliset ja kansainväliset sotilaalliset ja siviilialojen toimet, joilla puolustetaan Suomen valtiollista itsenäisyyttä sekä kansan turvallisuutta ulkoisia, valtioiden aiheuttamia *kyberuhkia* ja -*poikkeamia* vastaan

huomautus
Valtioiden aiheuttamia kyberuhkia ja -poikkeamia voivat toteuttaa myös sellaiset *kyberuhkatoimijat*, jotka eivät ole valtiollisia organisaatioita.

Siviilialojen toimiin kuuluvat muun muassa diplomatian, tiedustelun, informaation hallinnan ja strategisen viestinnän, rikostorjunnan ja finanssialan keinot sekä taloudelliset, oikeudelliset ja erilaiset *kyberturvallisuuden (1)* keinot.

Kansalliseen kyberpuolustukseen kuuluu myös tarvittavien vastatoimien toimeenpaneminen kaikissa valmiustiloissa sekä *kyberpelotteen* tuottaminen.

Eri sektorien toimijoiden kyberpuolustuksen toimista vastaavat eri hallinnonalojen viranomaiset.

Kansallinen kyberpuolustus kytkeytyy olennaisesti *kansalliseen kyberturvallisuuteen*.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

50
kyberpelote
sv cyberavskräckning
en cyber deterrence; cyberdeterrence

määritelmä
valtion strategia, jonka tarkoituksena on estää vihamielinen kybertoiminta vakuuttamalla *kyberuhkatoimijat* siitä, että hyökkäyksellä ei saavuteta tavoitteita tai se ei muutoin kannata

huomautus
Kyberpelote käsittää ne siviili- ja sotilasalojen keinot, joilla valtio suojaa *kybertoimintaympäristöä* ja aiheuttaa kustannuksia kyberuhkatoimijoille.

Kyberpelotteella suojataan valtion suvereniteettia kybertoimintaympäristössä. Se on osa valtion kokonaispelotetta.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

51
<Suomi>
sotilaallinen kyberpuolustus
sv militärt cyberförsvar *n*
en military cyber defence; military cyberdefence

määritelmä
toimet, joiden tarkoituksena on sotilaallisten *kyberoperaatioiden* toimeenpano sekä Suomen puolustuskykyyn vaikuttavien järjestelmien ja eri sektorien toimijoiden turvaaminen valtioiden aiheuttamilta *kyberuhkilta* ja -*poikkeamilta*

huomautus
Sotilaallinen kyberpuolustus muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä ja muista tukitoimista.

Sotilaallinen kyberpuolustus varmistaa Suomen puolustuskyvyn, toteuttaa tarvittavat vastatoimet ja turvaa valtion suvereniteetin *kybertoimintaympäristössä*.

Sotilaallinen kyberpuolustus on osa *kansallista kyberpuolustusta*.

Puolustusvoimat vastaa Suomen sotilaallisesta kyberpuolustuksesta, sen johtamisesta ja toteuttamisesta yhteistoiminnassa muiden viranomaisten ja sektorien kanssa.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

52
kyberoperaatio
sv cyberoperation
en cyber operation; cyberoperation; cyberspace operation <Nato>

määritelmä
suunnitelmallinen ja johdettu sarja pääosin *kybertoimintaympäristössä* tapahtuvia toimintoja, joilla pyritään suojaamaan kohde, hankkimaan siitä tietoa tai vaikuttamaan sen toimintaan

huomautus
Kyberoperaatio voi olla joko puolustuksellinen tai hyökkäyksellinen.

Kyberoperaation tueksi vaaditaan usein tiedustelu- ja muita tukitoimia, jotka eivät välttämättä tapahdu yksinomaan kybertoimintaympäristössä.

Kyberoperaatioon voi kuulua *kyberhyökkäyksiä*.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaaviot: Kyberhyökkäys ja Kybertoimintaympäristö ja siihen liittyvä toiminta

53
kyberkampanja; < kampanja
sv cyberkampanj
en cyber campaign

määritelmä
valtiolliseen toimintaan liittyvä, strategisilta tavoitteiltaan johdonmukainen ja usein pitkäkestoinen toiminta, johon kuuluu yksi tai useampi *kyberoperaatio* ja muita yhteensovitettuja toimia

huomautus
Kyberkampanja voi sisältää useita erilaisia, eri toimijoiden toteuttamia, eri toimijoihin kohdistettuja ja eri aikaan toteutettuja kyberoperaatioita. Toimijoina voi olla niin siviili- kuin sotilastoimijoita.

Kyberoperaatioiden lisäksi kyberkampanjaan voi kuulua esimerkiksi taloudellisia, diplomaattisia tai juridisia toimia ja muita *kybertoimintaympäristöön* liittyviä toimia.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

54
<kyberturvallisuus>
attribuutio
sv attribution; attribuering; tillskrivande
en attribution

määritelmä
prosessi, joka koostuu teknisten faktojen keräämisestä ja analysoimisesta sekä niiden kokonaisvaltaisesta tiedustelu-, ulko- ja turvallisuuspoliittisesta arvioinnista, ja jonka avulla tunnistetaan vihamielisen *kyberoperaation* tekijä sekä siitä vastuussa oleva taho

huomautus
Attribuutioksi voidaan toisinaan kutsua myös tehdyn ulko- ja turvallisuuspoliittisen päätöksen ulkoista viestintää.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

55
kybertiedustelu
sv cyberunderrättelser *pl*; inhämtning av cyberunderrättelser; cyberunderrättelseinhämtning
en cyberintelligence; cyber intelligence

määritelmä
julkisiin ja ei-julkisiin tiedonlähteisiin kohdistuva tiedonhankinta, jolla tuetaan *kyberturvallisuutta (1)* tai mahdollistetaan *kyberoperaatioiden* toteuttaminen

huomautus
Kybertiedustelua toteuttaa laaja joukko yksityisen ja julkisen sektorin toimijoita.

Kyberuhkatiedustelu on yksi kybertiedustelun osa-alueista.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

56
tietoverkkotiedustelu; verkkotiedustelu
sv underrättelseinhämtning som avser datanät; kränkning av informationssäkerhet /FI/; säkerhetsöverträdelseintrång *n*; > personuppgiftsincident
inte: signalspaning
en computer network and telecommunications intelligence
not: intelligence gathering on information networks; information networks intelligence; cyber intelligence

määritelmä
tietoverkossa oleviin lähteisiin kohdistuva tiedonhankinta, jonka tarkoituksena on kartoittaa ja lisätä ymmärrystä erilaisista uhkista, riskeistä, mahdollisuuksista ja muutoksista

huomautus
Tietoverkkotiedustelu koostuu tietoliikennetiedustelusta ja tietojärjestelmätiedustelusta.

Tietoverkkotiedustelua voi tapahtua niin maan sisällä kuin sen rajojen ulkopuolella.

Tietoverkkotiedustelu on yleensä valtioiden valtuuttamaa turvallisuus- ja tiedusteluviranomaisten toimintaa.

57
kyberdiplomatia
sv cyberdiplomati
en cyber diplomacy; cyberdiplomacy

määritelmä
kybertoimintaympäristöä koskevat ulko- ja turvallisuuspolitiikan keinot ja toimintatavat, joilla hoidetaan valtioiden välisiä suhteita sekä ehkäistään ja ratkaistaan konflikteja

huomautus
Kyberdiplomatian avulla kybertoimintaympäristöä koskevaa valtioiden välistä vuorovaikutusta ohjataan ja kehitetään yhteisten sääntöjen, normien ja yhteistyörakenteiden luomiseksi ja ylläpitämiseksi.

Kyberdiplomatia voidaan joissakin yhteyksissä nähdä laajempana käsitteenä, johon kuuluu myös muu valtioiden välinen yhteistyö *kyberturvallisuudessa (1)*, kuten *kyberrikollisuuden* ja muiden turvallisuusuhkien torjunta.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

58
kybersodankäynti; > tietoverkkosodankäynti
sv cyberkrigföring
en cyberwarfare; cyber warfare

määritelmä
kybertoimintaympäristössä tai sen välityksellä tapahtuva, valtioiden väliseen sodankäyntiin tai muuhun vakavaan konfliktiin liittyvä hyökkäyksellinen ja puolustuksellinen toiminta

huomautus
Kybersodankäynnin kaikki osapuolet eivät välttämättä ole valtiollisia toimijoita.

Termi kybersota ei ole kybersodankäynnin synonyymi, vaan se viittaa eri käsitteeseen. Kybersota on käsitteenä kiistanalainen, koska sotaa ei voi rajata vain yhteen toimintaympäristöön.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

59
kyberturvallisuuden kansallinen yhteistoimintamalli; kyberturvallisuuden yhteistoimintamalli
sv nationell samarbetsmodell för cybersäkerhet; samarbetsmodell för cybersäkerhet
en national cooperation model for cybersecurity; cybersecurity cooperation model

määritelmä
toimintatapa, jolla varmistetaan yhteiskunnan keskeisten toimijoiden tiivis yhteistyö varautumisessa kaikissa oloissa ja siten yhteiskunnan kyky ennakoida, ehkäistä ja havainnoida *kyberpoikkeamia*, sietää niitä ja toipua niistä

huomautus
Kyberturvallisuuden kansallinen yhteistoimintamalli Suomessa vastaa periaatteiltaan kokonaisturvallisuuden yhteistoimintamallia.

Kyberpoikkeamiin varaudutaan ja niihin reagoidaan tiiviissä yhteistyössä julkisen sektorin, elinkeinoelämän ja kansalaisyhteiskunnan kanssa.

Kyberturvallisuuden kansallinen yhteistoimintamalli on kuvattu Yhteiskunnan turvallisuusstrategiassa (Valtioneuvoston julkaisuja 2025:1).

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*. Cybersecurity voidaan kirjoittaa myös erikseen (cyber security).

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta

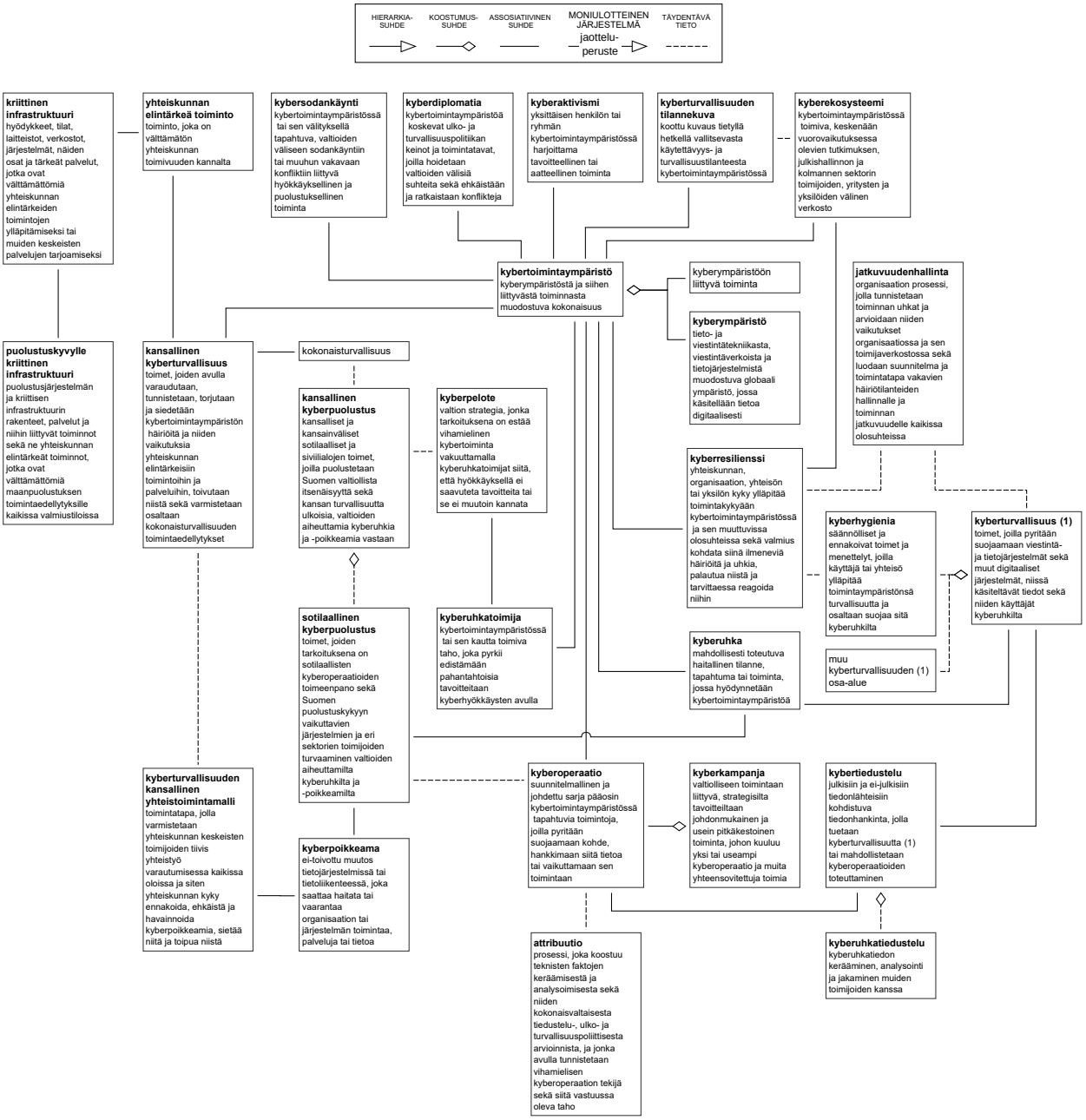
60
kyberaktivismi; ~ haktivismi
sv cyberaktivism; ~ hacktivism
en cyber activism; cyberactivism; ~ hacktivism

määritelmä
yksittäisen henkilön tai ryhmän *kybertoimintaympäristössä* harjoittama tavoitteellinen tai aatteellinen toiminta

huomautus
Kyberaktivismilla voidaan tavoitella huomiota tai muutosta johonkin asiaan. Se voi olla joko hyvän- tai pahantahtoista toimintaa.

Englannin kielen cyber-alkuisten termien erikseen- tai yhteenkirjoittaminen vaihtelee, ks. *kyber-*.

Käsitejärjestelmäkaavio: Kybertoimintaympäristö ja siihen liittyvä toiminta



Käsitejärjestelmäkaavio 4. *Kybertoimintaympäristö ja siihen liittyvä toiminta.*

Englanninkielinen hakemisto / English index

Numbers in the index refer to the term record numbers.

Ruotsinkielinen hakemisto / Svenskt register

Numren i registret anger termpostnumren.

Suomenkielinen hakemisto

Hakemiston numerot viittaavat termitietuenumeroihin.