Turvallisuuskomitea
Säkerhetskommittén
The Security Committee

KYBERTURVALLISUUDEN SANASTO

Ordlista om cybersäkerhet

Vocabulary of Cyber Security

2018

Viestintävirasto
Kyberturvallisuuskeskus

tsk SANASTOKESKUS TSK
TERMINOLOGICENTRALEN TSK

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

SANASTOKESKUS TSK
TERMINOLOGICENTRALEN TSK

TSK 52

KYBERTURVALLISUUDEN SANASTO

Ordlista om cybersäkerhet

Vocabulary of Cyber Security

2018

Julkaisija: Sanastokeskus TSK ry
Kustantaja: Huoltovarmuuskeskus
Toimeksiantaja: Turvallisuuskomitea

ISBN 978-952-5608-49-6 (Huoltovarmuuskeskus)
ISSN 1795-6323 (Sanastokeskus TSK ry)

Helsinki 2018

Sanastokeskus TSK
Runeberginkatu 4c B 20, 00100 Helsinki
tsk@tsk.fi
www.tsk.fi

Huoltovarmuuskeskus
Aleksanterinkatu 48 A, 00100 Helsinki
www.huoltovarmuuskeskus.fi

Turvallisuuskomitea
Puolustusministeriö
Eteläinen Makasiinikatu 8, PL 31, 00131 Helsinki
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

Esipuhe

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.

Kokonaisturvallisuuden sanastossa (TSK 50) on määritelty joitakin kyberturvallisuuteen liittyviä käsitteitä, ja myös *Suomen kyberturvallisuusstrategiassa* (valtioneuvoston periaatepäätös 24.1.2013) annetaan muutamien keskeisten kyberturvallisuus- ja tietoturvakäsitteiden määritelmät. Lisäksi eri organisaatiot ovat laatineet aiheeseen liittyviä sanastoja, mutta laajaa suomenkielistä kyberturvallisuussanastoa ei ole aiemmin julkaistu.

Turvallisuuskomitean sihteeristö ja Huoltovarmuuskeskus käynnistivät Sanastokeskus TSK:n kanssa toukokuussa 2017 projektin, jonka tavoitteena oli koota sanasto, joka selvittää keskeisten kyberturvallisuus- ja tietoturvakäsitteiden sisällöt ja antaa tarvittavat suositukset suomenkielisestä termistöstä. Sanastoprojekti oli samalla osa Suomen kansallisen kyberturvallisuusstrategian toimeenpanoa.

Projektin tuloksena syntyneessä *Kyberturvallisuuden sanastossa* (TSK 52) on esitetty termitietueina ja käsitekaavioina noin 70:n aihepiiriin kuuluvan käsitteen tiedot. Koska kyberturvallisuuteen liittyy tiiviisti tietoturva, on sanastoon sisällytetty myös keskeisiä tietoturvakäsitteitä. Käsitteiden sisältö on kuvattu määritelmien ja niitä täydentävien lisätietojen avulla. Käsitteiden välisiä suhteita havainnollistetaan käsitekaavioiden avulla. Lisäksi termeille annetaan vastineet ruotsin ja englannin kielillä.

Kyberturvallisuuden sanaston tavoitteena on selventää käsitteitä, yhdenmukaistaa termejä ja antaa luotettavia vieraskielisiä vastineita suomen kielen käsitteille ja helpottaa alalla työskentelevien tai muuten kyberturvallisuuden kanssa tekemisiin tulevien työtä. Sanasto on tarkoitettu käytettäväksi muun muassa opetustoiminnassa, kansainvälisen yhteistyön tukena ja käytännön varautumistyössä.

Kyberturvallisuuden sanasto on toteutettu yhteistyössä eri hallinnonalojen kanssa. Sanastotyötä on ohjannut Turvallisuuskomitean sihteeristö ja sen rahoituksesta on vastannut Huoltovarmuuskeskus.

Kyberturvallisuuden sanastoa laatineeseen asiantuntijaryhmään ovat kuuluneet:

Pentti Olin, Turvallisuuskomitean sihteeristö, puheenjohtaja
Maarit Koivuniemi, valtiovarainministeriö
Martti Lehto, Jyväskylän yliopisto
Kalle Luukkainen, Huoltovarmuuskeskus
Noora Magd, puolustusvoimien tutkimuslaitos
Nadja Nevaste, Turvallisuuskomitea
Sami Niinikorpi, Suojelupoliisi
Johanna Rautio, Viestintävirasto
Mari Ristolainen, puolustusvoimien tutkimuslaitos
Marko Sjöroos, valtioneuvoston kanslia
Jussi Tuovinen, puolustusvoimien tutkimuslaitos
Päivi Kouki, Sanastokeskus TSK, terminologi
Sirpa Suhonen, Sanastokeskus TSK, terminologi

Sanaston ruotsin- ja englanninkielisten termivastineiden työstämiseen ovat osallistuneet seuraavat valtioneuvoston kanslian käännös- ja kielitoimialan kieliasiantuntijat:

Niina Elomaa
Merja Fleming
Anu Leppänen
Peter Ovell
Anita Strandberg
Katri Suvanto
Irma Talonen
Ursula Vuorenlinna

Sanastohankkeen lausuntokierroksen aikana kommentteja pyydettiin julkisen Lausuntopalvelu-portaalin kautta. Määräaikaan mennessä saapui yhteensä 15 lausuntoa viranomaisilta, järjestöiltä, tiedeyhteisöiltä ja yksityishenkilöiltä.

Sisällysluettelo

Käsitekaavioluettelo

Sanaston rakenne ja merkinnät

Käsitteet, määritelmät ja termit

Sanaston lähtökohtana on ollut luotettavien määritelmien, käsitejärjestelmien ja termivastineiden 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. **Tarkoitteet** voivat olla konkreettisia (esim. *hakkeri*) tai abstrakteja (esim. *kriittinen infrastruktuuri*), ja niillä on erilaisia ominaisuuksia (esimerkiksi *kriittinen infrastruktuuri* tarkoittaa perusrakenteita, palveluja ja niihin liittyviä toimintoja, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi). 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 kullakin sanaston kielellä. Hakemistoihin on poimittu suositettavien ja hylättävien termien lisäksi muita hakusanoja, jotka liittyvät läheisesti tiettyyn käsitteeseen. Muut hakusanat viittaavat siihen käsitteeseen ja sen numeroon, jonka yhteydessä sanaa käsitellään.

Termitietueen rakenne

Käsitteet on esitetty sekä numeroituina termitietueina että käsitejärjestelmiä kuvaavina kaavioina. Käsitekaaviot ja termitietueet on tarkoitettu toisiaan tukeviksi esitysmuodoiksi. Kaikki sanaston käsitteet eivät ole mukana kaavioissa.

Termitietueessa käsitteille annetaan ensin **suomenkieliset termit**. Jos käsite on määritelty, termien jälkeen seuraa suomenkielinen **määritelmä** ja mahdolliset määritelmää täydentävät lisätiedot eli **huomautukset**. Käsitteet on numeroitu juoksevasti. Alla on esimerkkinä käsitettä *kyberhäiriötilanne* käsittelevä termitietue ja merkintöjen selitykset:

38		käsitteen numero
kyberhäiriötilanne; kyberturvallisuuden häiriötilanne; kyberhäiriö		suomenkieliset termit; suositettavin ensimmäisenä, jos termejä on useita
sv	cyberstörningssituation; störningssituation i cybersäkerheten; cyberstörning	ruotsinkieliset vastineet, suositettavin ensimmäisenä
en	cyber incident; cyber security incident	englanninkieliset vastineet, suositettavin ensimmäisenä, jos termejä on useita
toteutunut *kyberuhka*, joka haittaa organisaation tai järjestelmän toimintaa		määritelmä (alkaa pienellä kirjaimella, ei pistettä lopussa, kursivointi viittaa sanastossa määriteltyyn käsitteeseen)
	Kyberhäiriötilanteiden hallinta voidaan jakaa eri osa-alueisiin, joita ovat esimerkiksi varautuminen, tilannekuvan muodostaminen, torjunta ja palautuminen.	huomautus (normaali virke, erotettu määritelmästä sisennyksellä, antaa lisätietoa käsitteestä, esimerkkejä, tietoa termien käytöstä yms.)

Kooste kaikista käsitteiden yhteydessä sanasto-osuudessa käytetyistä merkintätavoista:

lihavointi	suomenkielinen suositettava termi (ensimmäisenä suositettavin ja sen jälkeen hyväksyttävät synonyymit)
kursivointi	määritelmässä tai huomautuksessa: viittaus tässä sanastossa määriteltyyn käsitteeseen
(1)	suluissa oleva numero termin perässä: homonyymi; sanastossa on useita kirjoitusasultaan samanlaisia termejä, joilla on eri merkitys, esim. *it-krigföring (1)* ja *it-krigföring (2)*
mieluummin kuin: hellre än: rather than:	termin käyttöä ei suositeta kielellisistä syistä (esim. vierasperäisyyden vuoksi)
ei: inte: not:	termi tarkoittaa eri asiaa kuin suositettava termi, eikä sitä pitäisi käyttää tässä merkityksessä, tai termi on kielen-vastainen
†	termi on vanhentunut
sv	ruotsinkieliset vastineet (suositettavin ensin)
en	englanninkieliset vastineet (suositettavin ensin)
/FI/	suomenruotsia
/US/	Yhdysvaltain englantia
n	ruotsin termi on ett-sukuinen
pl	termiä käytetään monikkomuotoisena
<	termi tai vastine viittaa määriteltyä käsitettä laajempaan käsitteeseen
>	termi tai vastine viittaa määriteltyä käsitettä suppeampaan käsitteeseen
~	termi tai vastine viittaa hieman määritellystä käsitteestä poikkeavaan käsitteeseen, mutta siitä ei kuitenkaan voi sanoa, että se olisi laajempi tai suppeampi kuin määritelty käsite
(tietoaineisto-turvallisuudesta)	teksti kaarisuluissa termin perässä: täsmennys termin käyttöalasta tai tapauksista, joissa termiä voidaan käyttää
<kyberturvallisuus>	teksti kulmasuluissa käsitteen numeron alla: ala, jolle määritelmä on rajattu tai jonka näkökulmasta määritelmä on kirjoitettu
Käsitekaavio: Kyberuhkat	viittaus käsitekaavioon, jossa käsite esiintyy

Käsitekaavioiden tulkinta

Käsitekaaviot 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). Seuraavan sivun kaaviossa on annettu esimerkkejä käsitesuhteiden kuvaamisesta.

Käsitteen merkitseminen kaavioon

- sanasto-osuudesta käsitteen tiedoista on poimittu kaavioon käsitteen numero, 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 (*tietoverkkohyökkäys*) ja sitä suppeamman alakäsitteen (*palvelunestohyökkäys*) 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 *kyberturvallisuus* koostuu *kyberpuolustuksesta* ja muista kyberturvallisuuden osa-alueista
- vinoneliö kiinnittyy yläkäsitteeseen

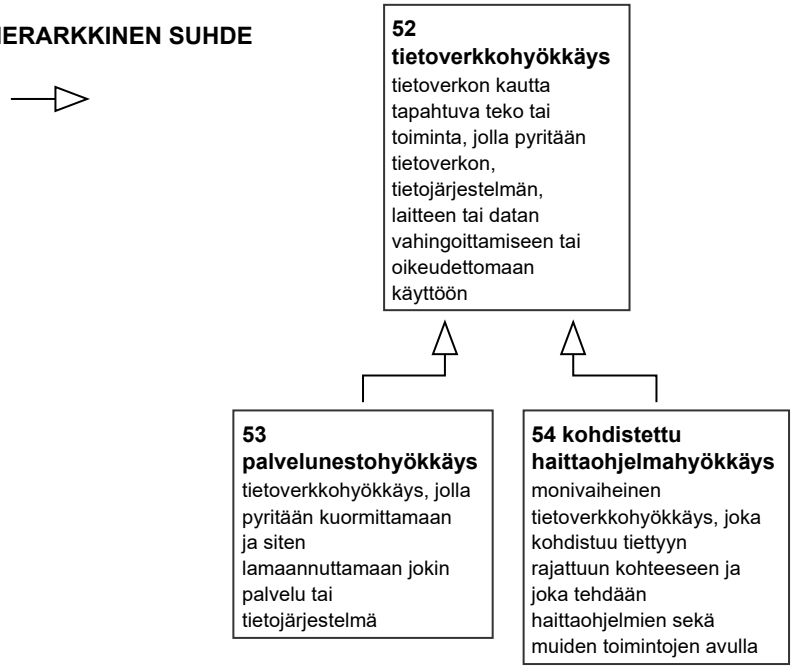
Assosiatiivinen suhde (viiva ilman symbolia)

- käsitesuhde, jota ei voida luokitella hierarkkiseksi tai koostumussuhteeksi (esim. ajalliset, paikalliset, toiminnalliset, välineelliset sekä alkuperään ja syntyyn liittyvät suhteet)
- assosiatiivisen suhteen tyyppi käy yleensä ilmi määritelmän kielellisestä muodosta
- esimerkiksi *tietoturvan* ja *haavoittuvuuden* välillä on assosiatiivinen suhde: haavoittuvuus tarkoittaa alttiutta tietoturvaan kohdistuville uhkille

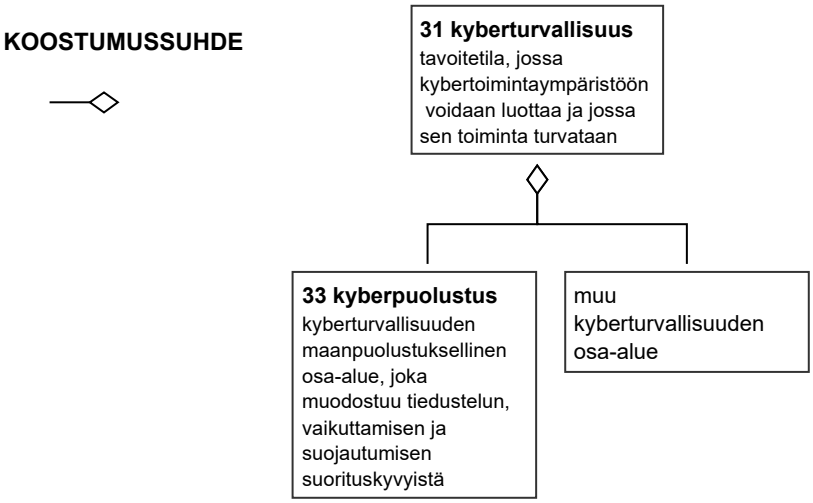
Katkoviivoilla kuvattu käsitesuhde

- katkoviivoilla merkitään käsitesuhteet, jotka eivät käy ilmi määritelmien sanamuodoista (esimerkiksi käsitteiden *kyberpuolustuksen* ja *tietoverkkotiedustelun* välinen koostumussuhde on merkitty katkoviivalla, koska tietoverkkotiedustelun määritelmässä ei viitata suoraan *kyberpuolustukseen* eikä päinvastoin)
- katkoviivoilla kuvatut käsitesuhteet täydentävät määritelmiä ja tukevat käsitteiden ymmärtämistä (*tietoverkkotiedustelu* on yksi *kyberpuolustuksen* osa-alue, vaikka koostumussuhde ei näy käsitteiden määritelmistä)
- katkoviivalla voidaan merkitä niin hierarkkinen suhde, koostumussuhde kuin assosiatiivinen suhdekin

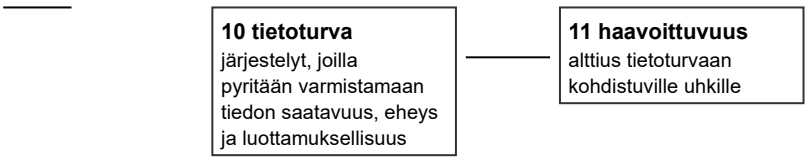
HIERARKKINEN SUHDE



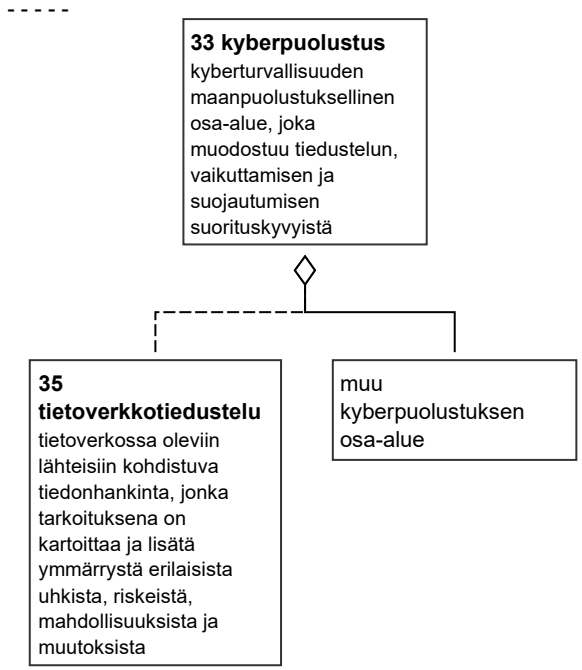
KOOSTUMUSSUHDE



ASSOSIATIIVINEN SUHDE



KATKOVIIVALLA KUVATTU TÄYDENTÄVÄ TIETO



1 YLEINEN TURVALLISUUS

1
riski
sv risk
en risk

määritelmä
epävarmuuden vaikutus tavoitteisiin

huomautus
Vaikutus on poikkeama odotetusta. Se voi olla myönteinen, kielteinen tai molempia, ja se voi käsitellä, luoda tai saada aikaan mahdollisuuksia ja uhkia.

Riski ilmaistaan tavallisesti riskin lähteiden, mahdollisten tapahtumien, niiden seurausten ja niiden todennäköisyyden yhdistelmänä.

Riskit voivat kohdistua esimerkiksi ihmisiin, eläimiin, omaisuuteen, tietojärjestelmiin, ympäristöön tai yhteisöllisiin arvoihin.

Yleiskielessä sekä suomen kielen sanan "riski" että ruotsin- ja englanninkielisten vastineiden merkitys on kielteinen.

2
suojattava kohde; turvattava kohde
sv objekt *n* som ska skyddas
en asset to be protected

määritelmä
yhteiskunnan tai organisaation toiminnan kannalta merkityksellinen kohde, joka halutaan suojata *riskien* varalta

huomautus
Suojattava kohde voi olla esimerkiksi tieto, tietojärjestelmä, prosessi, fyysinen tila, yksittäinen asiakirja tai työasema.

3
turvallisuusluokitusmerkintä; turvaluokitusmerkintä
sv anteckning om säkerhetsklassificering
en security classification marking

määritelmä
erityinen merkintä joka tehdään salassa pidettävään viranomaisen asiakirjaan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta

huomautus
Turvallisuusluokitusmerkintä voidaan tehdä asiakirjaan siinä tapauksessa, jos asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle *viranomaisten toiminnan julkisuudesta annetun lain (621/1999)* 24 §:n 1 momentin 2 ja 7–10 kohdassa tarkoitetulla tavalla.

Turvallisuusluokitusmerkintää ei saa käyttää muissa kuin edellä mainitun lain 1 momentissa tarkoitetuissa tapauksissa, ellei merkinnän tekeminen ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön.

4
Kansallinen turvallisuusauditointikriteeristö; Katakri
sv Nationell kriteriesamling för säkerhetsauditering; Katakri
en National Security Auditing Criteria; Katakri

määritelmä
viranomaisten käyttöön tarkoitettu arviointityökalu, jonka avulla voidaan arvioida kohdeorganisaation kykyä suojata viranomaisen turvallisuusluokiteltua tietoa

huomautus
Kansallista turvallisuusauditointikriteeristöä voidaan käyttää arvioitaessa organisaation turvallisuusjärjestelyjen toteutumista yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Lisäksi sitä voidaan käyttää apuna yrityksien, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja sen kehittämisessä.

Kansallinen turvallisuusauditointikriteeristö perustuu *valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010)* ja *EU:n turvallisuusluokiteltujen tietojen suojaamista koskeviin turvallisuussääntöihin (2013/488/EU)*.

5
turvallisuusselvitys
sv säkerhetsutredning
en security clearance

määritelmä
Suojelupoliisin tai puolustusvoimien tekemä selvitys henkilön taustasta tai organisaation vastuuhenkilöistä, *tietoturvan* tasosta ja sitoumusten hoitokyvystä

huomautus
Turvallisuusselvityslain (762/2014) mukaan selvityksen laatimisen yleisenä edellytyksenä on, että selvityksen kohde on antanut siihen etukäteen kirjallisen suostumuksen.

Turvallisuusselvityksen päätyttyä selvityksen kohteesta voidaan antaa turvallisuusselvitystodistus.

Henkilöturvallisuusselvitys voidaan tehdä henkilöstä, joka työskentelee erityistä luottamusta vaativissa tehtävissä tai joka työtehtävissään voi merkittävällä tavalla vaarantaa valtion turvallisuutta. Selvityksen kattavuus vaihtelee sen mukaan, onko kyseessä suppea, perusmuotoinen vai laaja henkilöturvallisuusselvitys.

Henkilöturvallisuusselvitystä hakee pääsääntöisesti työnantaja tai muu sellainen taho, jonka antamaa työtä tai toimeksiantoa selvityksen kohteena olevan henkilön on tarkoitus hoitaa.

Yritysturvallisuusselvitys voidaan tehdä suomalaisesta organisaatiosta, joka toimii viranomaisen sopimuskumppanina ja tarvitsee oikeuden käsitellä turvallisuusluokiteltuja viranomaistietoja.

6
yhteiskunnan elintärkeä toiminto
sv samhällets vitala funktioner *pl*; vitala samhällsfunktioner *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 (ks. *resilienssi*).

Käsitekaavio: *Kyberturvallisuus*

7
kriittinen infrastruktuuri
sv kritisk infrastruktur
en critical infrastructure; CI

määritelmä
perusrakenteet, palvelut ja niihin liittyvät toiminnot, jotka ovat välttämättömiä *yhteiskunnan elintärkeiden toimintojen* ylläpitämiseksi

huomautus
Kriittiseen infrastruktuuriin kuuluu sekä fyysisiä laitoksia ja rakenteita että digitaalisia toimintoja ja palveluja. Muun muassa energian tuotanto-, siirto- ja jakelujärjestelmät, liikenne ja logistiikka, tieto- ja viestintäjärjestelmät sekä vesi- ja jätehuolto ovat osa kriittistä infrastruktuuria.

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.

Käsitekaavio: *Kyberturvallisuus*

8
resilienssi; ~ kriisinkestävyys; ~ kriisinsietoisuus
sv resiliens; ~ kristålighet
en resilience; ~ crisis resilience; ~ crisis tolerance

määritelmä
yksilöiden ja yhteisöjen kyky ylläpitää toimintakykyä muuttuvissa olosuhteissa sekä valmius kohdata häiriöitä ja kriisejä ja palautua niistä

huomautus
Resilienssin lähtökohtana on ajatus siitä, että turvallisuutta vaarantavat tilanteet syntyvät toimintojen odottamattomista yhdistelmistä, eivät niinkään toimintavirheistä tai häiriöistä, joita voidaan hallita suunnittelulla. Turvallisuuden hallinta onnistuu, jos toimintatavat joustavat tilanteiden ja olosuhteiden mukaisesti. Resilienssiin liitettyjä määreitä ovat joustavuus, kimmoisuus ja palautumiskyky.

Termiä resilienssi käytetään osin samassa merkityksessä kuin termiä kriisinkestävyys.

9
jatkuvuudenhallinta
sv kontinuitetshantering; hantering av kontinuitet
en continuity management; > business continuity management

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

huomautus
Jatkuvuudenhallinta on organisaation ylimmän johdon hyväksymää strategista ja operatiivista toimintaa, jolla organisaatio varautuu hallitsemaan häiriötilanteet ja jatkamaan toimintaa ennalta määritellyllä hyväksyttävällä tasolla. Jatkuvuuden hallinta on *resilienssin* osa-alue.

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

2 TIETOTURVA

10

tietoturva; tietoturvallisuus

sv informationssäkerhet; it-säkerhet; > datasäkerhet (datamängder)

en < information security; > data security (data sets)

määritelmä

järjestelyt, 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.

Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen.

Tietoturvalla ja tietoturvallisuudella voidaan tarkoittaa myös oloja, joissa tietoturvariskit ovat hallinnassa.

Käsitekaaviot: *Tietoturva*

11

haavoittuvuus

sv sårbarhet; utsatthet; känslighet

en vulnerability

määritelmä

alttius *tietoturvaan* kohdistuville uhkille

huomautus

Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa.

Nollapäivähaavoittuvuus on tietojärjestelmässä oleva haavoittuvuus, johon ei ole saatavilla korjausta.

Käsitekaaviot: *Tietoturva*

12

henkilötietosuoja; tietosuoja

sv integritetsskydd *n*; skydd *n* för personuppgifter; sekretesskydd; sekretess

en privacy protection; confidentiality of personal information /US/; data protection

määritelmä

järjestelyt, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen

huomautus

Henkilötietosuoja pyritään toteuttamaan muun muassa *tietoturvalla*. Aikaisemmin tietosuoja-sanan merkitys on ymmärretty laajemmin käsittämään muutakin kuin henkilötietojen suojaamista.

Käsitekaavio: *Tietoturva*

13
tietoturvatapahtuma; tietoturvallisuustapahtuma
sv informationssäkerhetshändelse; it-händelse
en information security event

määritelmä
tietojärjestelmän tai organisaation toimintojen tapahtuma, jonka seurauksena tietojen tai palvelujen tila on muuttunut ja joka saattaa vaikuttaa *tietoturvaan*

huomautus
Tietoturvatapahtumia voidaan havaita esimerkiksi tunnistamalla muutoksia tai poikkeamia (engl. anomalies) datassa tai tietojärjestelmän toiminnassa. Muutoksia ja poikkeamia havaitaan pääasiassa teknisiä työkaluja hyödyntävillä seulonnoilla.

Ks. myös *tietoturvahäiriö*.

Käsitekaavio: *Tietoturva*

14
tietoturvahäiriö; tietoturvapoikkeama
sv informationssäkerhetsincident; it-säkerhetsincident; it-incident
en information security incident

määritelmä
yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu *tietoturvatapahtuma*, joka vaarantaa tietojen ja palvelujen *tietoturvan* ja vaikuttaa organisaation toimintaan epäsuotuisasti

Käsitekaavio: *Tietoturva*

15
tietoturvahäiriön hallinta; tietoturvapoikkeaman hallinta
sv hantering av informationssäkerhetsincidenter; hantering av it-incidenter; it-incidenthantering
en information security incident management; incident management; information security incident handling; ~ information security incident response

määritelmä
toimenpiteet, joilla varaudutaan ja reagoidaan *tietoturvahäiriöihin* vahinkojen rajoittamiseksi ja niistä toipumiseksi

Käsitekaavio: *Tietoturva*

16
tietoturvavalvomo; tietoturvahallintakeskus
sv säkerhetsoperationscenter *n*
en security operations centre; SOC; information security operations centre; ISOC

määritelmä
organisaatio tai sen osa, jossa muodostetaan, seurataan ja analysoidaan *tietoturvan* tilannekuvaa, ehkäistään, tunnistetaan ja analysoidaan *tietoturvahäiriöitä*, dokumentoidaan niitä sekä reagoidaan niihin ohjeistuksen mukaisesti

huomautus
Organisaatiolla voi olla oma tietoturvavalvomo tai valvomon palvelut voidaan ostaa ulkopuoliselta palveluntarjoajalta.

Käsitekaavio: *Tietoturva*

17
tietoturvaloukkaus
sv säkerhetsöverträdelse; kränkning av informationssäkerheten /FI/; ~ brott mot informationssäkerheten; < säkerhetsbrott *n*; > brott *n* mot datasäkerhet; > personuppgiftsincident
en security breach; security violation
not: data breach

määritelmä
oikeudeton puuttuminen tietoon tai tietojärjestelmään

huomautus
Yleisimpiä tietoturvaloukkauksia ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, haittaohjelmatartunta, *palvelunestohyökkäys*, tietojen varastaminen ja *kohdistetut haittaohjelma-hyökkäykset*.

Käsitekaavio: *Tietoturva*

18
tietoturvaloukkauksen tutkinta
sv utredning av säkerhetsöverträdelse; utredning av informationssäkerhetsbrott; utredning av datasäkerhetsbrott
en investigation of information security breach; information security breach investigation; ~ digital forensics

määritelmä
toimenpiteet, jotka käynnistetään *tietoturvaloukkauksen* paljastuttua loukkauksen selvittämiseksi

huomautus
Tietoturvaloukkauksen tutkinta voi käsittää muun muassa todistusaineiston turvaamista, forensiikkaa, haittaohjelma-analyysia, lokianalyysia tai yleisesti tietoturvaloukkauksen vaikutusten ja laajuuden selvittämistä.

Käsitekaavio: *Tietoturva*

19
tietoverkkovalvomo; verkkovalvomo
sv nätövervakningscentral; nätverksoperationscenter *n*
en network operations centre; NOC; internet network operations centre; INOC; network management centre

määritelmä
organisaatio tai sen osa, jossa hallinnoidaan ja valvotaan yhtä tai useampaa tietoverkkoa

Käsitekaavio: *Tietoturva*

20
pääsynhallinta
sv åtkomsthantering
hellre än: accesshantering
en access management; AM

määritelmä
menettelyt, joilla varmistetaan, että käyttäjät, laitteet, sovellukset ja järjestelmät pääsevät käyttämään tietojärjestelmissä olevaa tietoa roolinsa mukaisesti

Käsitekaavio: *Tietoturva*

21
identiteetinhallinta
sv identitetshantering
en identity management; IdM

määritelmä
menettelyt, joilla hallinnoidaan käyttäjien ja laitteiden tunnuksia, rooleja ja ryhmiä

Käsitekaavio: *Tietoturva*

22
käyttöoikeuksien hallinta
sv åtkomstkontroll
hellre än: accesskontroll
en access control

määritelmä
menettelyt, joilla myönnetään, evätään tai muilla tavoin käsitellään käyttöoikeuksia palveluihin ja järjestelmäresursseihin

huomautus
Järjestelmäresursseja ovat esimerkiksi tiedostot ja tietoliikenneyhteydet.

Käsitekaavio: *Tietoturva*

23
todentaminen; todennus
mieluummin kuin: autentikointi
sv autentisering; verifiering; kontroll
en authentication; verification

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

huomautus
Kyberturvallisuuden 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.

Vrt. *tunnistus*.

Käsitekaavio: *Tietoturva*

24
monivaiheinen todentaminen; monivaiheinen todennus; monimenetelmäinen todentaminen; monimenetelmäinen todennus
sv multifaktorautentisering; MFA
en multi-factor authentication; MFA; multi-step verification

määritelmä
todentaminen vähintään kahta eri menetelmää käyttäen

Käsitekaavio: *Tietoturva*

25
tunnistus; tunnistaminen
sv identifiering; identifikation; igenkänning
en recognition; identification

määritelmä
menettely, jolla varmistetaan henkilön identiteetti tai esineen tai asian tunniste

huomautus
Tunnistus voi perustua tunnistautumiseen tai olla passiivista tunnistamista, joka ei edellytä tunnistettavalta toimintaa ja jossa tunnistettava henkilö ei välttämättä tiedä tulevansa tunnistetuksi.

Henkilön tunnistus perustuu siihen, mitä henkilö tietää (esimerkiksi salasana), mitä henkilöllä on hallussaan (esimerkiksi passi) tai kuka henkilö on (sormenjälki tai muu käyttäjän yksilöivä ominaisuus).

Vrt. *todentaminen*.

Käsitekaavio: *Tietoturva*

26

sähköinen henkilöllisyys; sähköinen identiteetti; digitaalinen identiteetti; sähköinen henkilötunnistetieto

sv elektronisk identitet

en electronic identity; electronic ID; digital identity; digital ID

määritelmä

yksilöivä tieto, jonka perusteella luonnollinen tai oikeushenkilö on todennettavissa digitaalisessa toimintaympäristössä

Käsitekaavio: *Tietoturva*

27

<tietoturva>

käyttäjän manipulointi

sv social manipulering; social manipulation

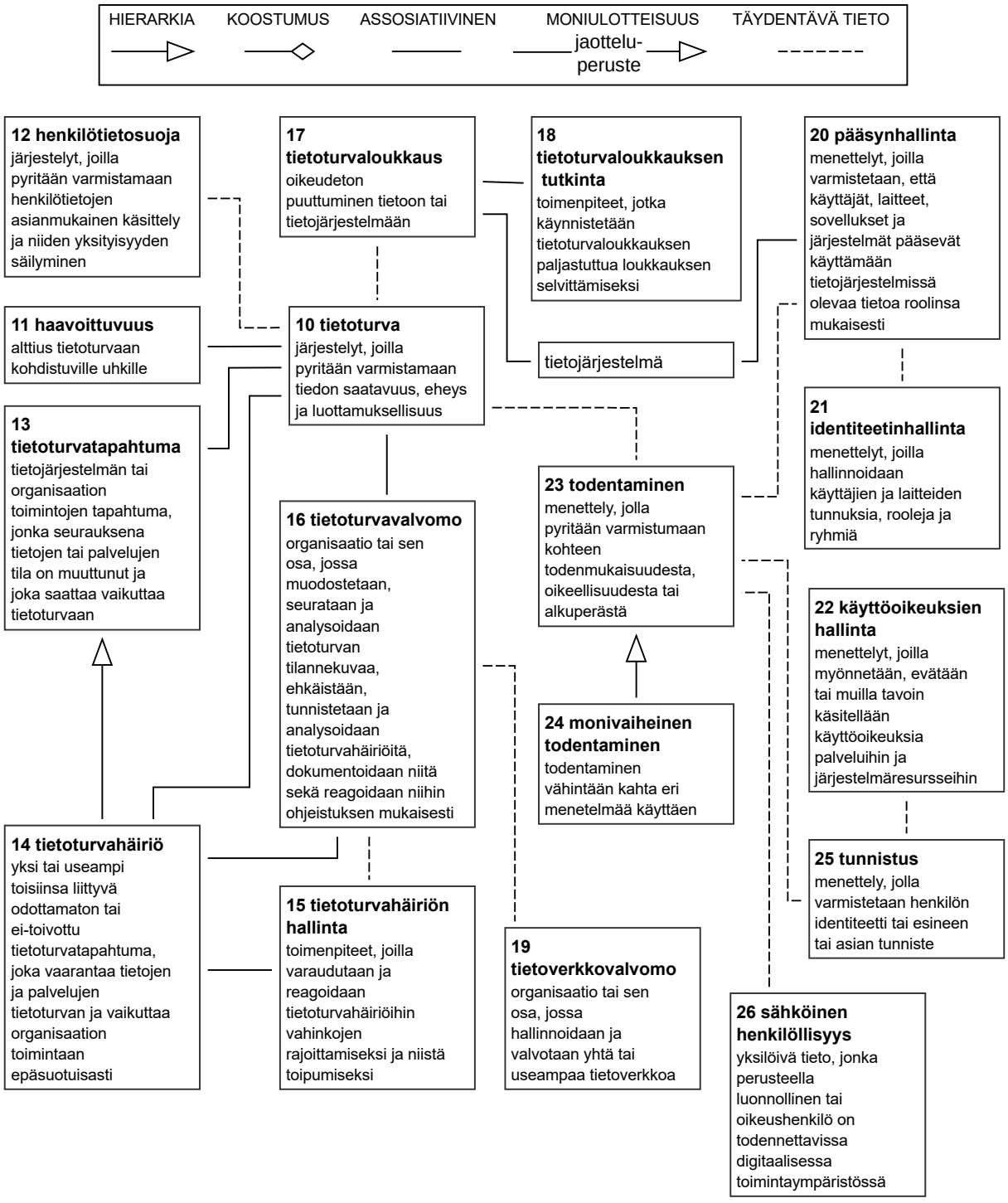
en social engineering

määritelmä

toiminta, jonka tavoitteena on hankkia luottamuksellista tietoa tekeytymällä tiedon käyttöön oikeutetuksi ja käyttämällä hyväksi tiedon käyttöön oikeutettuja henkilöitä

huomautus

Käyttäjän manipulointi voi kohdistua yhteen tai useampaan henkilöön. Usein manipuloinnilla pyritään selvittämään käyttäjän salasana.



Käsitekaavio 1. *Tietoturva.*

3 KYBERTURVALLISUUS

28

kyber-

sv cyber-

en cyber

huomautus

Kyber-sanaa käytetään yleensä yhdyssanan määriteosana. Sanan merkityssisältö liittyy yleensä digitaalisessa muodossa olevan informaation käsittelyyn: tietotekniikkaan, digitaaliseen viestintään (tietoverkkoihin), tietojärjestelmiin tai tietokonejärjestelmiin. 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.

29

kybertoimintaympäristö; kyberympäristö

sv cybermiljö; < cyberrymd

en cyber environment; < cyberspace; > cyber domain

määritelmä

yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö

huomautus

Kybertoimintaympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet.

Esimerkkejä kybertoimintaympäristöistä ovat tietojärjestelmiin perustuvat ydinvoimalan ohjausjärjestelmä, elintarvikkeiden kuljetus- ja logistiikkajärjestelmä, liikenteen ohjausjärjestelmät sekä pankki- ja maksujärjestelmät.

Englannin kielen termi ”cyber domain” viittaa sotilaalliseen kybertoimintaympäristöön.

Käsitekaaviot: *Kyberturvallisuus* ja *Kyberuhkat*

30

kyberturvallisuuslaboratorio; kyberlaboratorio

sv laboratorium *n* för cybersäkerhet

en cyber security laboratory

määritelmä

julkisista verkoista eristetty todenmukainen tietojärjestelmäympäristö, jossa voidaan toteuttaa tietoturvatestausta tai *kyberuhkien* torjumiseen liittyviä harjoituksia

huomautus

Suomessa on useita kyberturvallisuuslaboratoriota, esimerkiksi korkeakouluissa ja tutkimuslaitoksissa.

31
kyberturvallisuus
ei: kybersuojaus
sv cybersäkerhet
en cyber security; cybersecurity

määritelmä
tavoitetila, jossa *kybertoimintaympäristöön* voidaan luottaa ja jossa sen toiminta turvataan

huomautus
Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia *kyberuhkia* ja niiden vaikutuksia.

Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta *tietoturvauhkasta*, joten kyberturvallisuuteen pyrittäessä *tietoturva* on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot.

Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.

Keskeiset tavoitteet ja toimintalinjat, joiden avulla Suomi vastaa kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistaa sen toimivuuden, määritellään Suomen kyberturvallisuusstrategiassa (valtioneuvoston periaatepäätös 24.1.2013).

Käsitekaaviot: *Kyberturvallisuus*

32
kyberturvallisuuden tilannekuva; kybertilannekuva
sv lägesbild över cybersäkerheten
en cyber security situational picture; cyber security situation picture; < cyber security situation awareness

määritelmä
koottu kuvaus tietojärjestelmien tietyllä hetkellä vallitsevasta käytettävyys- ja turvallisuustilanteesta sekä *kybertoimintaympäristön* vallitsevasta tilasta

huomautus
Kyberturvallisuuden tilannekuvaa tuotetaan päätöksenteon tueksi ja se perustuu havaintoihin, arviointeihin, mittareihin ja analyyseihin.

Kyberturvallisuuden tilannekuvaa voidaan tarkastella taktisella, operatiivisella tai strategisella tasolla.

Kyberturvallisuuden tilannekuvaa tuotetaan usein yhteistyössä eri toimijoiden kesken.

Viestintäviraston Kyberturvallisuuskeskus kokoaa ja koordinoi kansallista kyberturvallisuuden tilannekuvaa.

Käsitekaavio: *Kyberturvallisuus*

33
kyberpuolustus
sv cyberförsvar *n*
en cyber defence

määritelmä
kyberturvallisuuden maanpuolustuksellinen osa-alue, joka muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä

huomautus
Kyberpuolustuksesta vastaa Suomessa puolustusvoimat.

Käsitekaaviot: *Kyberturvallisuus*

34

tietoverkkovalvonta; verkkovalvonta

ei: kybervalvonta; massavalvonta

sv nätövervakning; nätverksövervakning; övervakning av nätverk

en network surveillance

määritelmä

toiminta, jossa seurataan ja analysoidaan omissa tietoverkoissa tapahtuvaa tietoliikennettä

huomautus

Organisaatiot voivat seurata ja analysoida oman tietoverkkonsa tietoliikennettä esimerkiksi teknisen vian tai virheen havaitsemiseksi tai *tietoturvasta* huolehtimiseksi.

Käsitekaavio: *Kyberturvallisuus*

35

tietoverkkotiedustelu; verkkotiedustelu

sv underrättelseinhämtning som avser datanät /FI/; underrättelseinhämtning i nätet /FI/

inte: signalspaning

en intelligence gathering on information networks; information networks intelligence

määritelmä

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

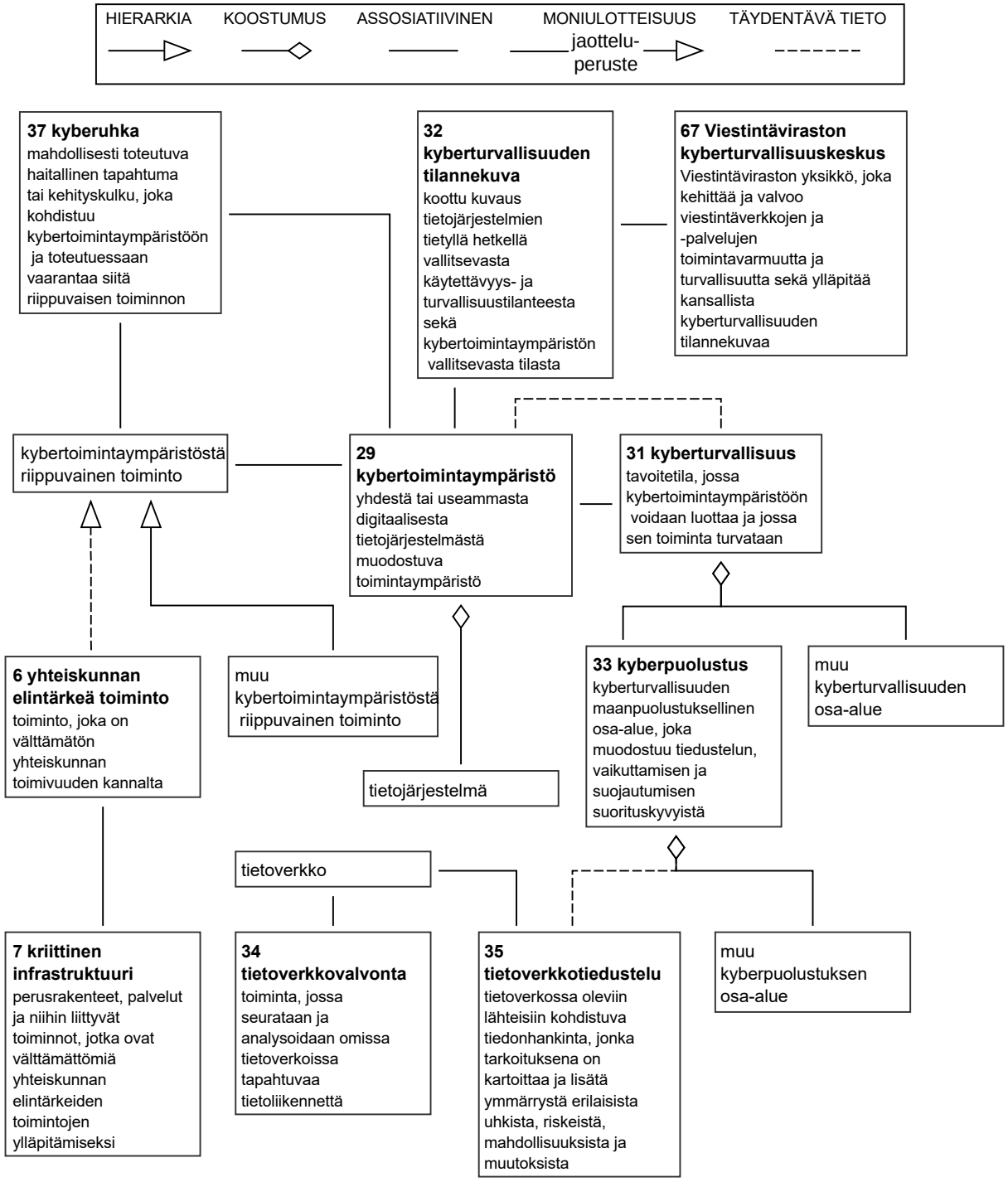
huomautus

Tietoverkkotiedustelu koostuu tietoliikennetiedustelusta ja tietojärjestelmätiedustelusta.

Tietoverkkotiedustelua voi tapahtua niin maan sisällä kuin rajojen ulkopuolella.

Tietoverkkotiedustelu on yleensä valtioiden valtuuttamaa toimintaa.

Käsitekaaviot: *Kyberturvallisuus*



Käsitekaavio 2. *Kyberturvallisuus.*

4 KYBERUHKAT

36

tietoturvauhka

sv hot *n* mot informationssäkerhet; informationssäkerhetshot *n*

en data security threat; information security threat

määritelmä

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

Käsitekaavio: *Kyberuhkat*

37

kyberuhka

sv cyberhot *n*

en cyber threat

määritelmä

mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu *kybertoimintaympäristöön* ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon

huomautus

Kyberuhkat voivat aiheutua paitsi toteutuneista *tietoturvauhkista* myös digitaalisessa viestintäympäristössä toteutettavista, yhteiskunnan turvallisuutta vaarantavista teoista.

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.

Esimerkkejä kybertoimintaympäristöistä riippuvaisista toiminnoista ovat ydinvoimalan ohjaus, elintarvikkeiden kuljetus ja logistiikka sekä liikenteen ohjaus.

Ks. myös *kyberturvallisuus*.

Käsitekaaviot: *Kyberturvallisuus* ja *Kyberuhkat*

38

kyberhäiriötilanne; kyberturvallisuuden häiriötilanne; kyberhäiriö

sv cyberstörningssituation; störningssituation i cybersäkerheten; cyberstörning

en cyber incident; cyber security incident

määritelmä

toteutunut *kyberuhka*, joka haittaa organisaation tai järjestelmän toimintaa

huomautus

Kyberhäiriötilanteiden hallinta voidaan jakaa eri osa-alueisiin, joita ovat esimerkiksi varautuminen, tilannekuvan muodostaminen, torjunta ja palautuminen.

Käsitekaavio: *Kyberuhkat*

39

kyberaktivismi; ~ haktivismi

sv cyberaktivism; ~ hacktivism

en cyber activism; ~ hacktivism

määritelmä

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

huomautus

Kyberaktivismilla voidaan tavoitella huomiota tai muutosta johonkin asiaan.

Kyberaktivistit voivat käyttää myös luonteeltaan rikollisia keinoja.

40
kybervandalismi
sv cybervandalism
en cyber vandalism

määritelmä
hakkerin tai hakkeriryhmän tekemä ilkivalta, jolla tekijä pyrkii aiheuttamaan vahinkoa tai hankkimaan mainetta

Käsitekaavio: *Kyberuhkat*

41
hakkeri
sv hackare
en hacker

määritelmä
henkilö, joka tunkeutuu tai vaikuttaa tietoverkkoon, tietojärjestelmään tai niiden sisältämään tietoon ja käyttää ohjelmaa, palvelua tai muuta resurssia

huomautus
Tunkeutuminen saattaa olla luvallista, esimerkiksi yritys voi palkata niin sanotun valkohattuhakkerin etsimään tietoverkostaan tai -järjestelmästään tietoturva-aukkoja tai *haavoittuvuuksia*.

Vihamielinen hakkeri saattaa esimerkiksi tuhota tietojärjestelmästä tietoja tai käyttää järjestelmää omiin tarkoituksiinsa.

Hakkeri-sanalla voidaan viitata myös taitavaan tietokoneharrastajaan.

42
kyberrikollisuus; tietoverkkorikollisuus
sv cyberbrottslighet; nätbrottslighet; cyberkriminalitet
en cybercrime

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

huomautus
Kyberrikollisuuden vaikutukset kohdistuvat tietojärjestelmien kautta niin valtioihin, yksityisiin kansalaisiin kuin organisaatioiden toimintaan.

Kyberrikoksia ovat esimerkiksi tietojen kalastelu, identiteettivarkaudet ja *palvelunestohyökkäykset*.

Käsitekaavio: *Kyberuhkat*

43
kybervakoilu; tietoverkkovakoilu
sv cyberspioneri; cyberspionage; nätspioneri; nätspionage
en cyber espionage; cyber spying

määritelmä
vakoilu, jossa hyödynnetään tietoverkkoja, niihin liitettyjä laitteita ja ohjelmistoja

huomautus
Kybervakoilu voi kohdistua valtioihin, yksityisiin kansalaisiin tai yrityksiin tai muihin organisaatioihin.

Kybervakoilussa voidaan käyttää hyväksi esimerkiksi *kohdistettuja haittaohjelmahyökkäyksiä*.

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

Käsitekaavio: *Kyberuhkat*

44
kyberterrorismi
sv cyberterrorism
en cyberterrorism

määritelmä
terroristinen toiminta, jossa hyökätään tietojärjestelmien kautta kansalaisia, liike-elämää, *yhteiskunnan elintärkeitä toimintoja* tai *kriittistä infrastruktuuria* tai muuta kohdetta vastaan

Käsitekaavio: *Kyberuhkat*

45
kyberoperaatio
sv cyberoperation
en cyber operation

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

huomautus
Kyberoperaatio voi olla joko puolustuksellinen tai hyökkäyksellinen. Sen tekijänä voi olla valtio, ryhmä tai yksittäinen henkilö.

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

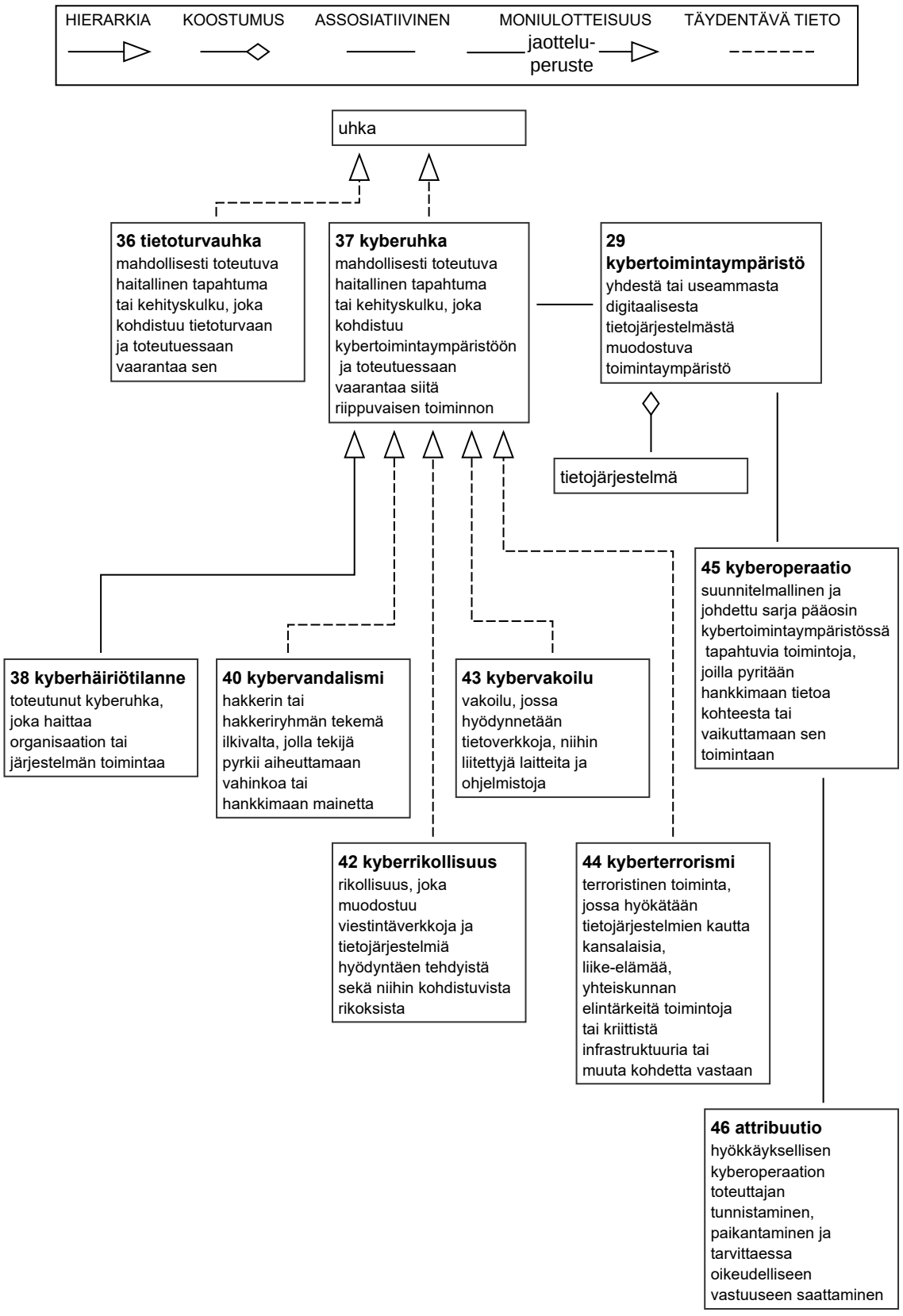
Käsitekaaviot: *Kyberuhkat* ja *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*

46
<kyberturvallisuus>
attribuutio
sv attribution
en attribution

määritelmä
hyökkäyksellisen *kyberoperaation* toteuttajan tunnistaminen, paikantaminen ja tarvittaessa oikeudelliseen vastuuseen saattaminen

huomautus
Hyökkäyksellisen kyberoperaation toteuttaja käyttää usein kaapattuja tietokoneita, palvelimia ja muita verkkoon kytkettyjä laitteita. Tästä syystä toteuttajaa ei pystytä paikantamaan IP-osoitteen perusteella, mikä tekee tämän tunnistamisesta ja paikantamisesta vaikeaa. Lisäksi valtioiden erilaiset oikeudelliset käytännöt estävät hyökkäyksen toteuttajan saamisen lailliseen edesvastuuseen, vaikka tämä olisi tunnistettu ja paikannettu. Tätä kutsutaan attribuutio-ongelmaksi.

Käsitekaavio: *Kyberuhkat*



Käsitekaavio 3. *Kyberuhkat.*

47
hybridivaikuttaminen
sv hybridpåverkan
en hybrid operations *pl*

määritelmä
poliittisesti motivoitunut suunnitelmallinen toiminta, jolla pyritään saavuttamaan omat tavoitteet erilaisia, toisiaan täydentäviä keinoja käyttäen ja kohteen heikkouksia hyödyntäen

huomautus
Hybridivaikuttamisen keinot voivat olla esimerkiksi taloudellisia, poliittisia tai sotilaallisia. Keinoja voidaan käyttää samanaikaisesti tai siten, että ne seuraavat toisiaan.

Hybridivaikuttamista tehdään esimerkiksi *informaatio*-, *kyber*-, fyysisten ja taloudellisten operaatioiden avulla.

Hybridivaikuttamisen takana voi olla joko valtiollinen tai ei-valtiollinen toimija.

Vrt. *informaatiovaikuttaminen*.

Käsitekaavio: *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*

48
informaatiovaikuttaminen
sv informationspåverkan
en information operations *pl* (1); influencing through information

määritelmä
toiminta, jossa informaatiota tuottamalla, muokkaamalla tai sen saatavuutta rajoittamalla muutetaan kohteen käsityksiä tai toimintaa informaatio- ja mielipideympäristön kautta

huomautus
Informaatiovaikuttamista on monentasoista ja sitä voidaan tehdä esimerkiksi *informaatio-operaatioiden* avulla.

Vrt. *hybridivaikuttaminen*.

Englanninkielisten termien käyttö ei ole vakiintunut. Anglosaksisessa maailmassa myös informaatiovaikuttamisesta käytetään laajasti termejä "information warfare" ja "information war", mutta Suomessa pyritään yleensä tekemään ero sodankäynnin ja vaikuttamisen välillä.

Käsitekaavio: *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*

49
informaatio-operaatio
sv informationsinsats; informationsoperation
en information operation (2)

määritelmä
suunnitelmallinen sarja toimintoja, joilla tuetaan ja koordinoidaan vaikuttamista informaatioon ja informaatiojärjestelmiin määritetyn tavoitteen saavuttamiseksi

huomautus
Informaatio-operaation päämääränä on tuottaa hallittuja suoria tai epäsuoria vaikutuksia informaatioympäristöön. Informaatio-operaatioilla tuetaan oman päätöksenteon edellytyksiä ja heikennetään vastustajan tilannetietoisuutta ja tahtoa. Tarvittaessa vaikutetaan vastustajan suorituskykyihin, jotka tukevat päätöksentekoa.

Informaatio-operaatiossa voidaan käyttää lukuisia eri keinoja, kuten *kyberoperaatioita*, psykologisia operaatioita, harhauttamista ja kohteiden fyysistä tuhoamista.

Informaatio-operaatiossa voidaan vaikuttaa useiden eri viestintäkanavien kautta.

Ks. myös *informaatiovaikuttaminen*.

Englanninkielistä termiä käytetään usein monikkomuodossa.

Käsitekaavio: *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*

50
informaatiosodankäynti
mieluummin kuin: tietosodankäynti
sv informationskrigföring; it-krigföring (1)
en information warfare; info-warfare; I-warfare; IW

määritelmä
vihamielinen vaikuttaminen valitun kohteen päätöksentekoon, toimintakykyyn ja mielipiteisiin informaatioympäristön kautta sekä suojautuminen toisten vastaavilta vaikuttamisyrityksiltä

huomautus
Informaatiosodankäyntiä voi tapahtua yhteiskunnallisin, poliittisin, viestinnällisin, psykologisin, sosiaalisin, taloudellisin ja sotilaallisin keinoin kaikilla sodankäynnin tasoilla. Informaatiosodankäynnin keskeiset vaikuttamis- ja suojautumiskeinot ovat *tietoverkkosodankäynti*, elektroninen sodankäynti, psykologinen sodankäynti, fyysinen vaikuttaminen tiedustelu-, valvonta- ja johtamisjärjestelmään, operaatioturvallisuus ja harhauttaminen.

Informaatiosotaa voidaan käydä esimerkiksi valtioiden tai organisaatioiden välillä. Informaatiosodankäynti voi vaikuttaa varsinaisen suunnitellun kohteen ulkopuolellakin, kuten sivullisten henkilöiden tai organisaatioiden tietojenkäsittelyjärjestelmissä.

Informaatiosodankäyntiin voi kuulua esimerkiksi *informaatio-operaatioiden* suorittaminen.

Käsitekaavio: *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*

51
tietoverkkosodankäynti; kybersodankäynti
sv it-krigföring (2); cyberkrigföring
en cyberwarfare; information network warfare

määritelmä
tietoverkkoja ja niiden *haavoittuvuuksia* hyödyntävä, valtioiden välinen vihamielinen toiminta

huomautus
Tietoverkkosodankäynnin käsite on kiistanalainen, koska sotaa ei voi rajata vain yhteen toimintaympäristöön.

Käsitekaavio: *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*

52
tietoverkkohyökkäys; verkkohyökkäys; < kyberhyökkäys
sv it-angrepp *n*; nätangrepp *n*; < cyberangrepp *n*
hellre än: nätverksattack
en network attack; < cyber attack

määritelmä
tietoverkon kautta tapahtuva teko tai toiminta, jolla pyritään tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön

huomautus
Tietoverkkohyökkäys voidaan tehdä esimerkiksi *palvelunestohyökkäyksenä* tai *haittaohjelman* avulla.

Termi ”kyberhyökkäys” viittaa tietoverkkohyökkäystä laajempaan käsitteeseen, sillä kyberhyökkäys voidaan tehdä myös muilla tavoin kuin tietoverkon kautta.

Käsitekaaviot: *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*

53

palvelunestohyökkäys

sv överbelastningsangrepp *n*
hellre än: överbelastningsattack

en denial of service attack; DoS attack

määritelmä
tietoverkkohyökkäys, jolla pyritään kuormittamaan ja siten lamaannuttamaan jokin palvelu tai tietojärjestelmä

huomautus
Palvelunestohyökkäys voi esimerkiksi lamaannuttaa sähköpostin suurella määrällä sähköpostiviestejä taikka palvelimen tai reitittimen liian suurella määrällä palvelupyyntöjä.

Jos palvelunestohyökkäys tulee yhdestä IP-osoitteesta, se on suhteellisen helppo havaita ja torjua esimerkiksi palomuurin avulla. Siksi palvelunestohyökkäys on yleensä hajautettu palvelunestohyökkäys (engl. distributed denial of service attack, DDoS attack), eli se toteutetaan yhtä aikaa useista eri lähteistä. Hajautettuun palvelunestohyökkäykseen käytetään usein hyökkääjän tietoverkon kautta haltuunsa ottamista tietokoneista muodostuvaa bottiverkkoa.

Jos palvelu lamaantuu tahattomasti ilman, että taustalla on hyökkäystä, tästä voidaan käyttää palvelunestotilanne-termiä. Esimerkiksi suosittu verkkosivusto voi lamaantua hetkellisen ja normaalia suuremman kävijämäärän vuoksi. Sekä palvelunestohyökkäys että palvelunestotilanne voivat aiheuttaa palvelunestotilan.

Käsitekaaviot: *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*

54

kohdistettu haittaohjelmahyökkäys; kohdistettu hyökkäys; APT-hyökkäys

sv riktat sabotageprogram *n*; riktat angrepp *n*; avancerat långvarigt hot *n*; apt-angrepp *n*

en advanced persistent threat; APT; targeted malware attack; targeted attack

määritelmä
monivaiheinen *tietoverkkohyökkäys*, joka kohdistuu tiettyyn rajattuun kohteeseen ja joka tehdään *haittaohjelmien* sekä muiden toimintojen avulla

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

Kohdistetun haittaohjelmahyökkäyksen tekijä hakee usein kohteesta tietoja, joita hyväksikäyttäen haittaohjelma on mahdollista saada kohteen järjestelmiin. Hyökkääjä pyrkii toimimaan niin, että hyökkäystä ei huomata ja sen jäljet poistetaan tietojärjestelmistä hyökkäyksen lähteen selvittämisen vaikeuttamiseksi.

Kohdistetut haittaohjelmahyökkäykset ovat yleensä pitkäkestoisia ja niissä käytetyt haittaohjelmat saattavat olla yksilöllisesti suunniteltuja.

Kohdistettu haittaohjelmahyökkäys voi olla *kyberoperaatio* tai kyberoperaation osa.

Kohdistetut haittaohjelmahyökkäykset ovat yleensä APT-ryhmien suunnittelemia ja toteuttamia operaatioita. APT-ryhmä on organisoitunut hakkeriryhmä, joka toimii itsenäisesti tai valtiollisen toimijan ohjauksessa. APT-ryhmiä pyritään tunnistamaan analysoimalla niiden käyttämiä toimintatapoja ja tekniikoita.

Kohdistettuja haittaohjelmahyökkäyksiä kutsutaan usein kampanjoiksi.

Käsitekaaviot: *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*

55

haittaohjelma; haittakoodi

sv skadligt program *n*; skadlig programvara; sabotageprogram *n*; skadeprogram *n*

en malicious software; malware; malicious program

määritelmä
ohjelma, joka tarkoituksellisesti aiheuttaa tietojärjestelmän tai laitteen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa

huomautus
Haittaohjelmia ovat esimerkiksi virukset, madot ja troijalaiset sekä näiden yhdistelmät.

Käsitekaavio: *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*

56

kiristyshaittaohjelma; kiristysohjelma; lunnasohjelma

sv utpressningsprogram *n*

en ransomware

määritelmä

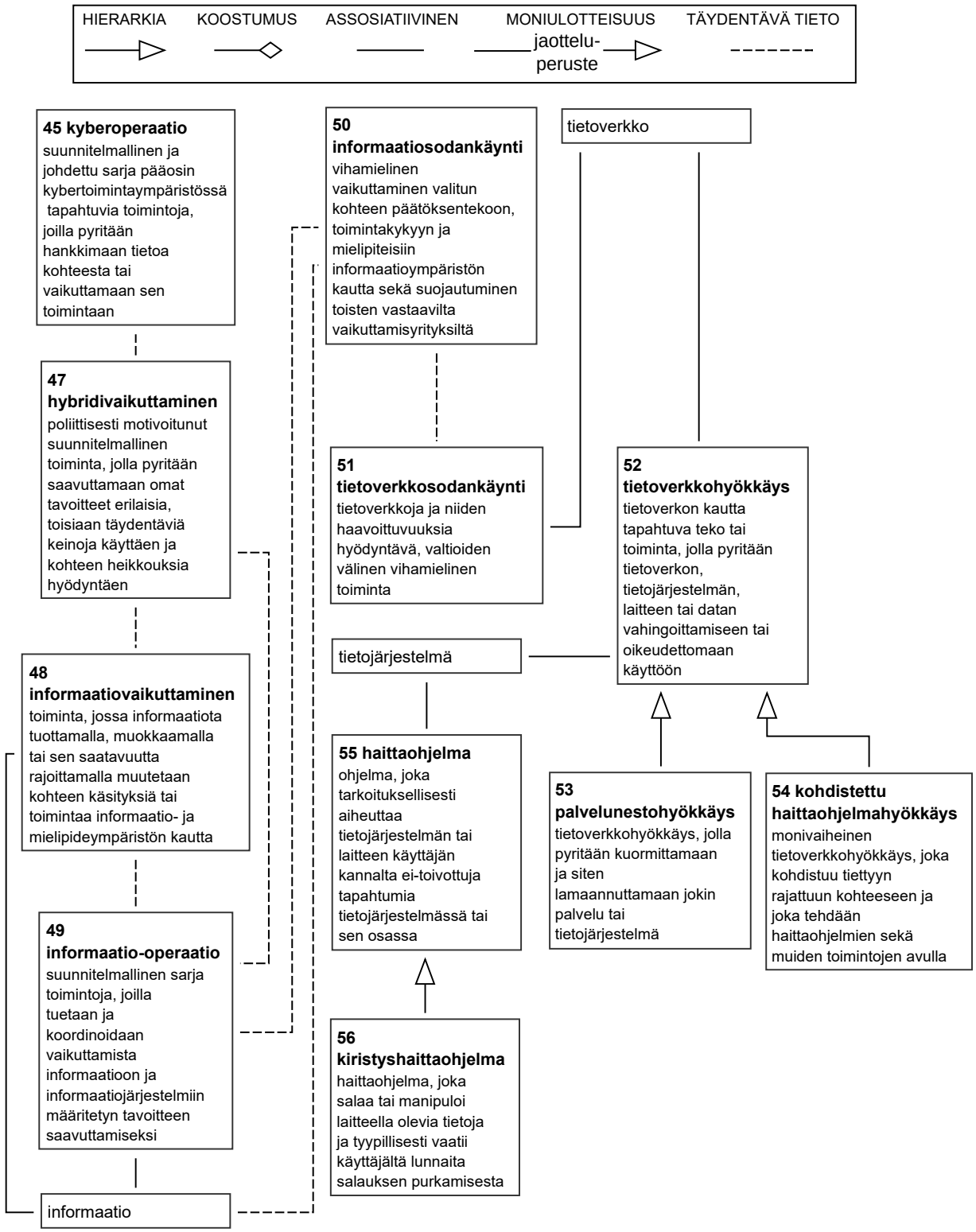
haittaohjelma, joka salaa tai manipuloi laitteella olevia tietoja ja tyypillisesti vaatii käyttäjältä lunnaita salauksen purkamisesta

huomautus

Kiristyshaittaohjelma voi tulla tietokoneeseen esimerkiksi sähköpostin liitetiedostona. Kun käyttäjä avaa liitetiedoston, kiristyshaittaohjelma latautuu koneelle, minkä jälkeen ohjelma esimerkiksi muuntaa joitakin tiedostoja salakirjoitettuun muotoon. Näitä tiedostoja ei voi avata ilman oikeaa salauksenpurkuavainta. Kiristyshaittaohjelman levittäjä lupaa toimittaa avaimen lunnaita vastaan.

Kiristyshaittaohjelma voi myös uhata levittää tai paljastaa luottamuksellista tietoa.

Käsitekaavio: *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat*



Käsitekaavio 4. *Informaatioon ja tietojärjestelmiin kohdistuvat uhkat.*

5 ORGANISAATIOT JA TOIMIJAT

57

Euroopan hybridiuhkien torjunnan osaamiskeskus; hybridiosaamiskeskus

sv Europeiska kompetenscentret *n* för motverkande av hybridhot

en European Centre of Excellence for Countering Hybrid Threats; Hybrid CoE

määritelmä

kansainvälinen osaamiskeskus, joka edistää hybridiuhkien torjuntaa parantamalla jäsenmaiden suorituskykyjä ja kehittämällä EU:n ja Naton yhteistyötä

huomautus

Euroopan hybridiuhkien torjunnan osaamiskeskuksen toiminta koostuu strategisen tason vuoropuhelusta, tutkimuksesta, koulutuksesta, konsultoinnista ja päätöksentekoharjoituksista.

58

hallinnon turvallisuusverkko; turvallisuusverkko; TUVE

sv förvaltningens säkerhetsnät *n*

en government security network

määritelmä

tietoverkko, jonka tarkoituksena on kaikissa turvallisuustilanteissa varmistaa valtion johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten ja muiden toimijoiden yhteistoiminnan edellyttämän viestinnän häiriöttömyys ja jatkuvuus sekä turvata päätöksenteossa ja johtamisessa tarvittavan tiedon *tietoturva*

huomautus

Hallinnon turvallisuusverkkoon kuuluvat viestintäverkko ja siihen välittömästi liittyvät laitetilat, laitteet ja muu infrastruktuuri sekä turvallisuusverkon yhteiset palvelut.

59

Havainnointi- ja varoitusjärjestelmä HAVARO; HAVARO

sv Nationellt observations- och varningssystem *n* (HAVARO)

en National Monitoring and Early Warning System (HAVARO)

määritelmä

erityisesti huoltovarmuuskriittisille organisaatioille suunnattu järjestelmä, joka havainnoi *tietoturvauhkia* ja varoittaa toteutuneista *tietoturvaloukkauksista* ja niiden yrityksistä

huomautus

HAVARO on Viestintäviraston tuottama ja *Huoltovarmuuskeskuksen* rahoittama järjestelmä, ja sen tarkoitus on kehittää huoltovarmuuskriittisten organisaatioiden kykyä varautua tietoturvauhkiin.

60

Huoltovarmuuskeskus; HVK

sv Försörjningsberedskapscentralen; FBC

en National Emergency Supply Agency; NESA

määritelmä

työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvä suunnittelu ja operatiivinen toiminta

61

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI; VAHTI

ei: † Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI

sv Ledningsgruppen för digital säkerhet inom den offentliga förvaltningen VAHTI; VAHTI
inte: † Ledningsgruppen för datasäkerheten inom statsförvaltningen VAHTI

en Public Sector Digital Security Management Board VAHTI; VAHTI
not: † Government Information Security Management Board VAHTI

määritelmä

valtionhallinnon elin, joka käsittelee ja sovittaa yhteen valtionhallinnon keskeiset *tietoturvan* ja *kyberturvallisuuden* linjaukset

huomautus

VAHTI on valtiovarainministeriön asettama ja toimii julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä.

VAHTI toimii Suomen kyberturvallisuusstrategian (valtioneuvoston periaatepäätös 24.1.2013) mukaisesti.

62

kansallinen kryptolaboratorio

sv nationell kryptologisk testmiljö

en National Cryptology Testing Environment

määritelmä

puolustusvoimien hallinnoima kansallinen tekninen ympäristö, jossa voi testata ja kehittää salausteknisiä ratkaisuja ja tuotteita

huomautus

Kansallinen kryptolaboratorio tukee muita viranomaisia salausratkaisujen arvioinnissa tarjoamalla käytännön testaus- ja todentamispalveluja. Lisäksi kryptolaboratorio tekee yhteistyötä tiedeyhteisön kanssa.

63

kansallinen turvallisuusviranomainen

sv nationell säkerhetsmyndighet

en National Security Authority; NSA

määritelmä

viranomainen, joka huolehtii kansainvälisten tietoturvavelvoitteiden toteuttamisesta ja valvoo, että kansainväliset turvallisuusluokitellut tietoaineistot suojataan ja että niitä käsitellään asianmukaisesti

huomautus

Kansallinen turvallisuusviranomainen koordinoi määrättyjen turvallisuusviranomaisten (Designated Security Authority, DSA) sekä kansallisen tietoturvallisuusviranomaisen (National Communications Security Authority, NCSA) toimintaa, osallistuu kansainvälisiin turvallisuuskomiteoihin ja -työryhmiin ja kansainvälisten turvallisuussääntöjen valmisteluun, neuvottelee kahden- ja monenvälisiä tietoturvasopimuksia sekä myöntää henkilö- ja yritysturvallisuustodistuksia kansainvälistä yhteistyötä varten.

Suomessa kansallisena turvallisuusviranomaisena toimii ulkoasiainministeriö.

Määrätyt kansalliset turvallisuusviranomaiset Suomessa ovat puolustusministeriö, Pääesikunta ja Suojelupoliisi, joille kullekin on jaettu omat vastuualueensa kansallisen turvallisuusviranomaisen kokonaisvastuukentässä.

Suomessa kansallisena tietoturvallisuusviranomaisena toimii *Viestintäviraston Kyberturvallisuuskeskuksen* NCSA-FI-ryhmä.

64

Kyberrikostorjuntakeskus

sv Centrum *n* mot cyberbrottslighet; Cyberbrottscentrum *n*

en Cybercrime Centre

määritelmä

Keskusrikospoliisin organisaation osa, jonka tehtäviin kuuluu vakavien kyberrikosten ennaltaehkäiseminen, paljastaminen ja selvittäminen

huomautus

Kyberrikostorjuntakeskus toimii kiinteässä yhteistyössä muiden poliisiyksiköiden kanssa *kyberrikollisuuden* torjumiseksi.

65

puolustusvoimien johtamisjärjestelmäkeskus; PVJJK

sv försvarsmaktens ledningssystemcenter *n*; FÖLSC

en Finnish Defence Forces C5 Agency; FDFC5A

määritelmä

Pääesikunnan alainen laitos, jonka tehtäviin kuuluu puolustusvoimien tietoteknisten palveluiden järjestäminen, ylläpitäminen ja *kyberpuolustus*

huomautus

Puolustusvoimien johtamisjärjestelmäkeskukseen kuuluu kyberosasto, joka ylläpitää puolustusvoimien *kyberturvallisuuden tilannekuvaa*, suojaa puolustusvoimien tietoverkkoja ja -palveluja sekä kehittää *kyberpuolustusta*.

66

Turvallisuuskomitea; TK

ei: † turvallisuus- ja puolustusasiain komitea; † TPAK

sv Säkerhetskommittén

inte: † säkerhets- och försvarskommittén

en Security Committee

määritelmä

puolustusministeriön yhteydessä toimiva, valtioneuvostoa ja ministeriöitä avustava komitea, joka on kokonaisturvallisuuden alalla varautumisen pysyvä yhteistoimintaelin ja tarvittaessa häiriötilanteissa asiantuntijaelin

huomautus

Turvallisuuskomitea seuraa Suomen turvallisuusympäristön ja yhteiskunnan kehitystä ja sekä osaltaan sovittaa yhteen kokonaisturvallisuuteen liittyvää ennakoivaa varautumista. Lisäksi Turvallisuuskomitea seuraa ja yhteensovittaa Suomen kyberturvallisuusstrategian (valtioneuvoston periaatepäätös 24.1.2013) toimeenpanoa.

67

Viestintäviraston kyberturvallisuuskeskus; Kyberturvallisuuskeskus

sv Kommunikationsverkets cybersäkerhetscenter; Cybersäkerhetscentret

en National Cyber Security Centre Finland; NCSC-FI

määritelmä

Viestintäviraston yksikkö, joka kehittää ja valvoo viestintäverkkojen ja -palvelujen toimintavarmuutta ja turvallisuutta sekä ylläpitää kansallista *kyberturvallisuuden tilannekuvaa*

huomautus

Viestintäviraston kyberturvallisuuskeskus tuottaa useita erilaisia tilannekuvatuotteita organisaatioille ja kansalaisille. Näitä ovat muun muassa varoitukset, haavoittuvuustiedotteet, tietoturva-aiheiset verkkojulkaisut ja toimialakohtaiset tietoturvatiedotteet.

Viestintäviraston kyberturvallisuuskeskuksessa toimii CERT-FI-ryhmä (Computer Emergency Response Team). CERT-FI:n tehtäviin kuuluu verkko-, viestintä- ja lisäarvopalveluihin kohdistuvien *tietoturvaloukkausten* ennaltaehkäisy, havainnointi ja ratkaiseminen, *tietoturvauhkista* ja -asioista tiedottaminen sekä tiedon kerääminen.

Käsitekaavio: *Kyberturvallisuus*

68

Väestörekisterikeskus; VRK

sv Befolkningsregistercentralen; BRC

en Population Register Centre

määritelmä

valtion virasto, joka toimii valtiovarainministeriön asettaman *Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTIn* toiminnasta vastaavana operatiivisena toimijana sekä kehittää yhteistyössä *Viestintäviraston Kyberturvallisuuskeskuksen* kanssa julkiseen hallintoon suunnattavia tieto- ja kyberturvallisuuspalveluita

huomautus

Väestörekisterikeskus myös tuottaa maksullisia digitaalisen turvallisuuden asiantuntijapalveluita julkisen hallinnon asiakkaille.

Englanninkielinen hakemisto / English index

Numbers in the index refer to the term record numbers.

Numbers in the index refer to the term record numbers.

Ruotsinkielinen hakemisto / Svenskt register

Numren i registret anger termpostnumren.

Numren i registret anger termpostnumren.

Suomenkielinen hakemisto

Hakemiston numerot viittaavat termitietuenumeroihin.

Hakemiston numerot viittaavat termitietuenumeroihin.