JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Informaatiovaikuttaminen

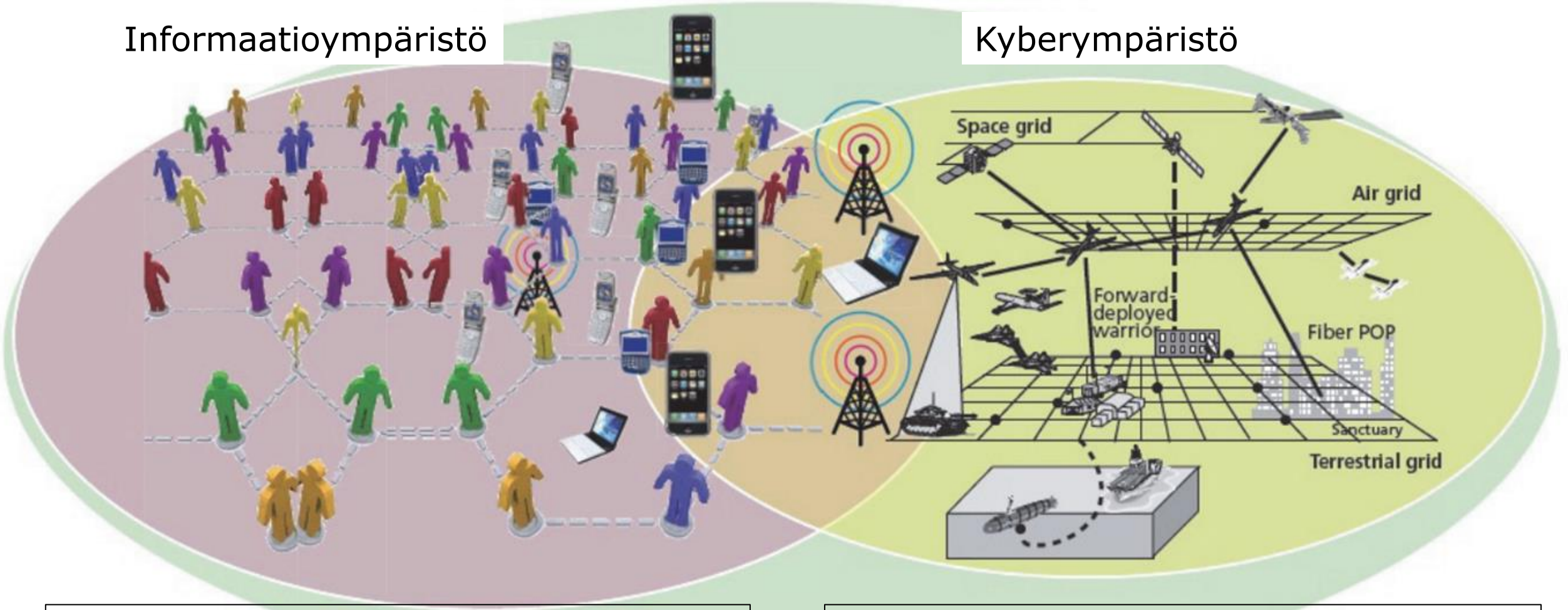
Työelämäprofessori, ST, eversti evp. Martti Lehto

8.6.2023

Esityksen sisältö

1. Kybermaailman kuvaus
2. Informaatiomaailman kuvaus
3. Haavoittuvuuksia
4. Uhkia
5. Turvallisuutta rakentamassa

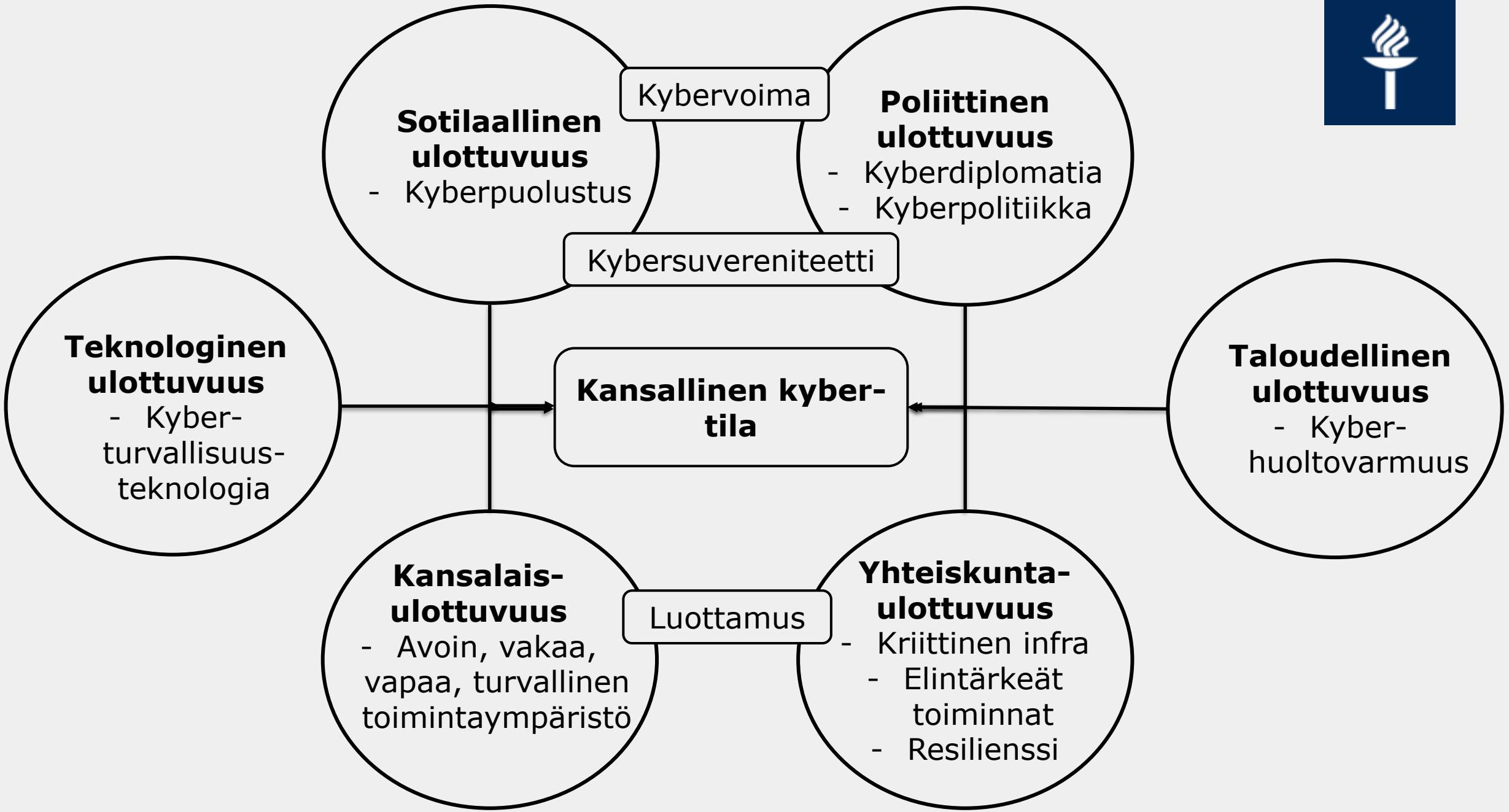
Kyberympäristö vs. Informaatioympäristö



Sosiaaliset verkostot muodostavat informaatioympäristön, jossa ilmenee yksilöiden välisten vuorovaikutusten ja suhteiden verkkoja.

Kyberympäristö on tekninen alusta tietojen vaihtamiseen, digitaalisiin palveluihin, tuotannon ja järjestelmien ohjaukseen ja liiketoimintaan.

Source: Isaac R. Porche III, Emerging Cyber Threats and Implications, The RAND Corporation, 2016


Kybervoima
Sotilaallinen ulottuvuus
- Kyberpuolustus
Poliittinen ulottuvuus
- Kyberdiplomatia
- Kyberpolitiikka
Kybersuvereniteetti
Teknologinen ulottuvuus
- Kyber-turvallisuus-teknologia
Kansallinen kyber-tila
Taloudellinen ulottuvuus
- Kyber-huoltovarmuus
Kansalais-ulottuvuus
- Avoin, vakaa, vapaa, turvallinen toimintaympäristö
Luottamus
Yhteiskunta-ulottuvuus
- Kriittinen infra
- Elintärkeät toiminnat
- Resilienssi

Kyberpolitiikka ja -diplomatia

Niin kansallisessa kuin kansainvälisessä politiikassa painottuu yhä enemmän kyberasioiden poliittinen luonne.

19 June 2017

Kyberpolitiikka ja -diplomatia

Pakotteet ovat yksi EU:n kyberdiplomatian välineistön keinoista torjua ja estää EU:hun tai sen jäsenmaihin kohdistuvia haitallisia kybertoimia ja vastata niihin.


European Council
Council of the European Union

Search

Home > Press > Press releases

Council of the EU Press release 30 July 2020 16:28

EU imposes the first ever sanctions against cyber-attacks

The Council today decided to impose **restrictive measures** against **six individuals** and **three entities** responsible for or involved in various **cyber-attacks**. These include the attempted cyber-attack against the **OPCW** (Organisation for the Prohibition of Chemical Weapons) and those publicly known as **'WannaCry'**, **'NotPetya'**, and **'Operation Cloud Hopper'**.

EU käytti tätä välineistöä ensimmäistä kertaa heinäkuussa 2020, kun neuvosto päätti määrätä rajoittavia toimenpiteitä useista kyberhyökkäyksistä vastuussa olevia tai niihin osallistuneita kuutta henkilöä (Kiina, Venäjä) ja kolmea yhteisöä (Kiina, Pohjois-Korea, Venäjä) vastaan.

Kybervoima

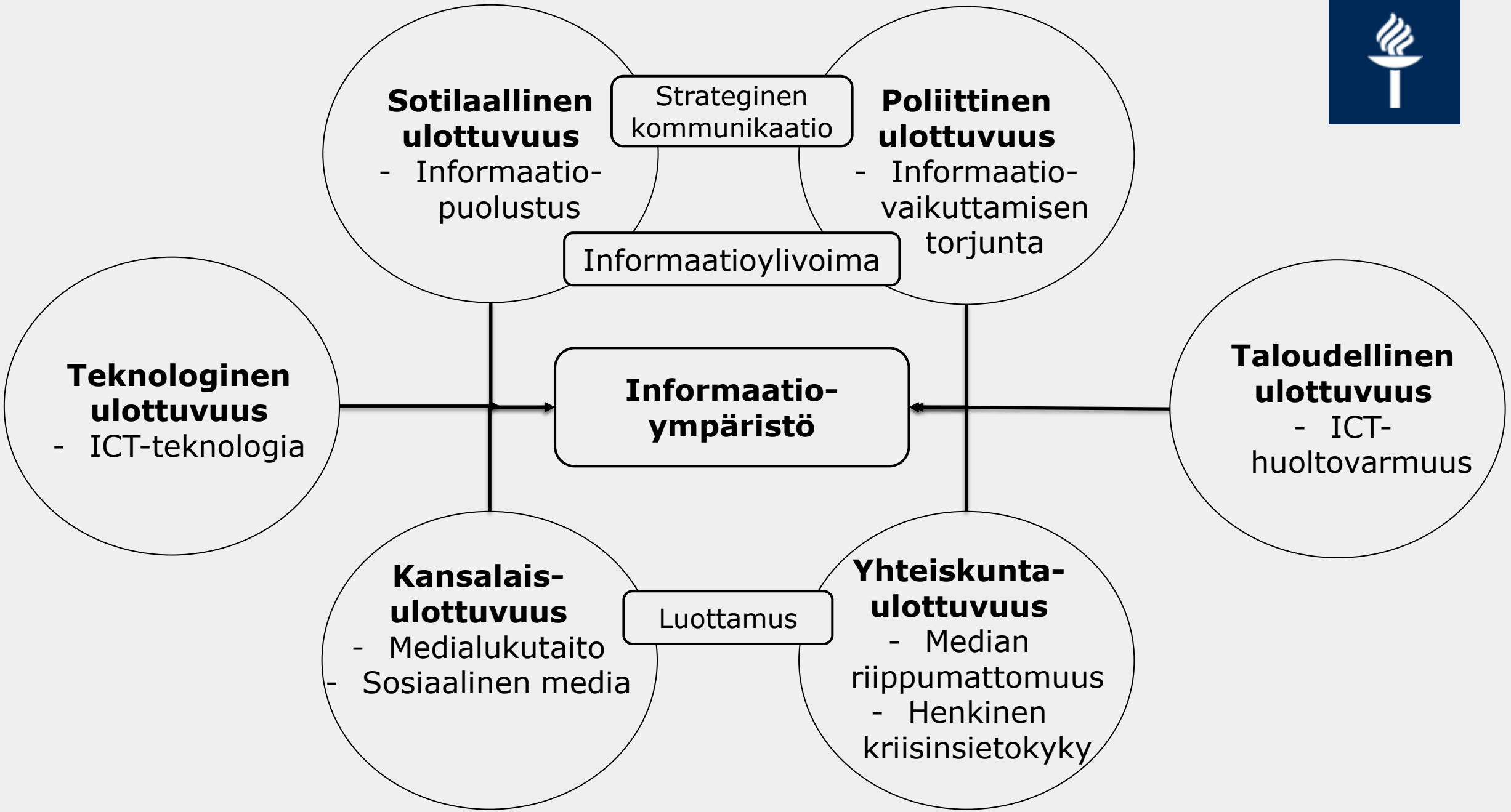
Kybervoima (Cyber Power) = kybersuorituskyvykkyydet vallankäytön välineinä, joka määrittää valtioiden roolin kybermaailmassa.

Harvardin Belfer National Cyber Power Index (NCPI) mittaa 30 maan kybervoimaa käyttäen 8 tavoitetta ja 29 suorituskykyindikaattoria.

Rank	2020	2022
1	US	US
2	China	China
3	UK	Russia
4	Russia	UK
5	Netherlands	Australia
6	France	Netherlands
7	Germany	ROK
8	Canada	Vietnam
9	Japan	France
10	Australia	Iran

Source: Harvard Kennedy School: National Cyber Power Index 2022 Belfer Center for Science and International Affairs, Sep 2022

Esityksen sisältö


Sotilaallinen ulottuvuus
- Informaatio-puolustus
Strateginen kommunikaatio
Poliittinen ulottuvuus
- Informaatio-vaikuttamisen torjunta
Informaatioylivoima
Teknologinen ulottuvuus
- ICT-teknologia
Informaatio-ympäristö
Taloudellinen ulottuvuus
- ICT-huoltovarmuus
Kansalais-ulottuvuus
- Medialukutaito
- Sosiaalinen media
Luottamus
Yhteiskunta-ulottuvuus
- Median riippumattomuus
- Henkinen kriisinsietokyky

Paikannus
-palvelut

Internet-
palvelut

Verkkopalvelu-tuottajat, ISP
Langalliset ja langattomat verkot

Ohjelmisto-tuottajat, ISWP
Microsoft, Apple, IBM, Oracle, SAP, Baidu…

Alustatuottajat, IPP
Palvelualustat: Google, Amazon, FB, Alibaba, Uber, Airbnb, eBay, Twitter…

Sisällön tuottajat, ICP
Yritykset, media, julkinen sektori, tutkimusyhteisö, kansalaiset…

Laitevalmistajat, IDP
Apple, Dell, Fujitsu, HP, Huawei, Lenovo Microsoft, Nokia Mitsubishi, Motorola, Samsung…

Internet-
verkkoja,
alustoja,
palveluita,
laitteita

Luottamuskriisi syvenee ja laajenee

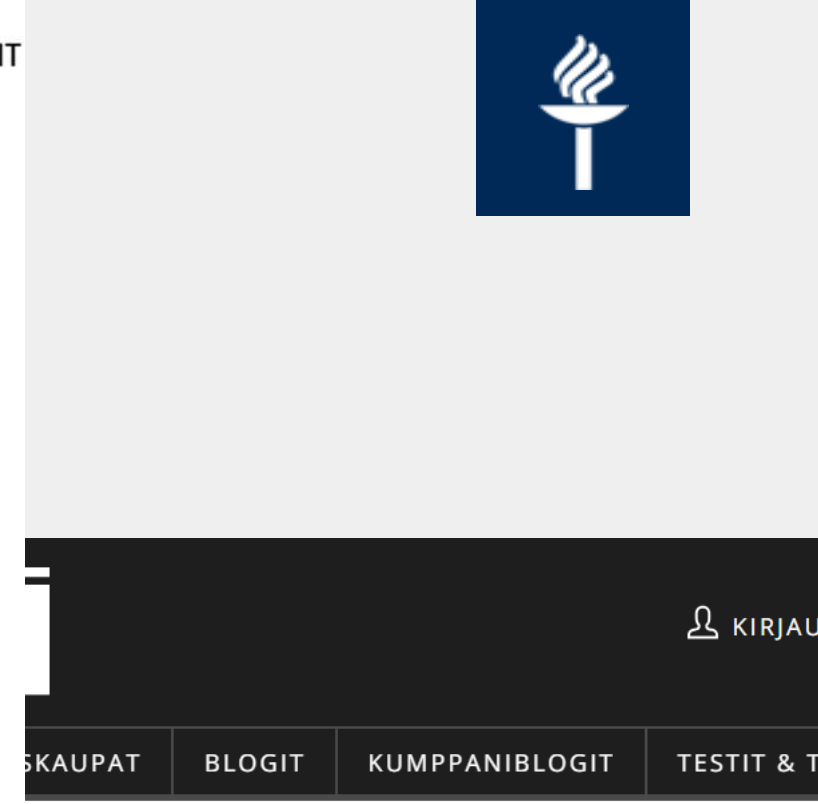
Euroopan parlamentti äänesti (13.6.2018) Kasperskyn olevan "ei-toivottu/haitallinen" (malicious) ja kieltää Kasperskyn tietoturvaohjelmistojen jäsenvaltioiden viranomaisten laitteistoissa kansallisen turvallisuuden nimissä. Kaspersky vastasi tähän lopettavansa kaiken yhteistyön kyberrikollisuuden torjunnassa Euroopan kanssa.

Presidentti Donald Trump allekirjoitti lain (15.8.2018), jonka seurauksena Yhdysvaltain valtionhallinto, urakoitsijat ja virastot joutuvat luopumaan suurelta osin Huawein ja ZTE:n valmistamasta teknologiasta.

Elokuussa 2018 Australian hallitus on päättänyt estää kiinalaisyhtiöitä osallistumasta maan 5g-verkkojen rakentamiseen. Päätös kohdistuu juuri Huawei-ZTE -kaksikkoon.

Jo aikaisemmin Huawei on suljettu ulos Australian valokuituverkon rakentamisesta ja Tyyneen mereen laskettavan datakaapelin toteuttamisesta.


Kauppalehti
UUTISET
PÖRSSI
YRITYKSET
JOHTAMINEN
OPTIO
TOIMITILAT
BLOGIT
Huawei heitettiin ulos puhelimien riskitietoja jakavasta järjestöstä – Ikävä uutinen laitteiden omistajille
21.9.2019 20:45
TIETOTURVA
DIGITALOUS
PUHELIMET
Android Authority kirjoittaa, että nyt on käynyt taas ovi yhdessä merkittävässä yhteistyöelimessä. Huawei ei enää saa olla mukana First-järjestössä (Forum of Incident Response and Security Teams). Jo parikymmentä vuotta toimineen järjestön puitteissa jäsenet vaihtavat tietoja haittaohjelmista, kyberturvallisuutta uhkaavista iskuista ja hakkerointitapauksista.
Tämä on ikävä uutinen Huawei-laitteiden omistajille. Tästedes kiinalaisyhtiö ei ole enää samalla viivalla muiden kanssa saamassa näitä tietoja tuoreina. Jos riskeistä joudutaan lukemaan vasta uutisista, vastatoimien kanssa ollaan auttamattomasti myöhässä.


KIRJAU
SKAUPAT
BLOGIT
KUMPPANIBLOGIT
TESTIT & T
Kiinalaisvalmistajia on epäilty takaovista – nyt Huawein laitteesta paljastui sellainen, mukana pikku yllätys
Ari Karkimo 4.4.2019 12:21 | päivitetty 4.4.2019 13:26 TIETOTURVA KIINA VAKOILU

INTERNET

Nyt se tapahtuu – Venäjä irtautuu internetistä

Jori Virtanen 11.2.2019 07:32 DIGITALOUS INTERNET

Joulukuussa 2018 hyväksytty laki velvoittaa Venäjän teleoperaattorit varmistamaan, että Runet toimii myös poikkeusoloissa.

Laki velvoittaa ohjaamaan kaiken internetliikenteen Venäjän Roskomnazorin hyväksymien tai sen hallitsemien solmujen läpi.

Roskomnazor estää kielletyn sisällön lataamisen ja varmistaa, että Venäjän kansalaisten internetliikenne pysyy Venäjän rajojen sisällä.

At the opening ceremony of the China 2nd World Internet Conference in 2015 president, Xi Jinping, set out his vision for the future of China's internet. **"We should respect the right of individual countries to independently choose their own path of cyber-development."**

Beijing wanted to ensure that internet content more actively served the interests of the Communist party.

Great Firewall (2013): yhdistelmä lain määräyksiä ja teknologiaa, jolla estetään halutun internet-liikenteen pääsyn Kiinaan.

Great Cannon (2015): pystyy säätämään ja korvaamaan Internetissä liikkuvia tietosisältöjä.

Kyber-maailma 2023

GPS	BeiDou	GLONASS
Yhdysvallat	**Kiina**	**Venäjä**
Google	Baidu Tieba	Yandex
WhatsApp	WeChat	Telegram
YouTube	Youku Tudou	RuTube
Amazon	AliBaba	Avito
Instagram	Nice, Meipai	Moi Mir
Twitter	Weibo	Futubra
Uber	DidiKuaidi	Yandex-Uber
Expedia	C-trip	Aviasales
Apple Pay	Alipay	Payonline
Wikipedia	Chinese Encyclopedia	Big Russian Encyclopedia
Facebook	Renren	Vkontakte, Odnoklassniki
Gmail/Hotmail/Yahoo	QQMail/AliMail	Mail.ru
Internet	China Net	RuNet

Määrittelyä

Informaatiosodankäynti

Informaatiosodankäynnissä pyritään vaikuttamaan informaation sisältöön ja kulkuun ja sitä kautta sodankäynnin tulokseen.

Käytettävät keinot voivat olla luonteeltaan strategisia, operatiivisia tai taktisia.

Informaatiosodankäynti

Tavoitteena on vaikuttaa sodan lopputulokseen.

Kohteina ovat:

- Vastustajan poliittinen ja sotilaallinen päätöksenteko: *Taipukaa tahtoomme*
- Vastustajan asevoimat ja kansa: *Henkinen lamauttaminen*
- Omat joukot ja kansa: *Henkisen kriisinsietokyvyn vahvistaminen ja toiminnan hyväksyttävyys*
- Ulkopuoliset: *Toiminnan hyväksyttävyyden vahvistaminen*

Kaikilla sodankäynnin tasoilla ja kaikissa sodan vaiheissa.

Informaatiovaikuttaminen

Toimintaa, jossa informaatiota tuottamalla, muokkaamalla tai sen saatavuutta rajoittamalla muutetaan kohteen käsityksiä tai toimintaa informaatio- ja mielipideympäristön kautta vaikuttajan hyödyksi.

Tämä on nyt käynnissä 24/7/365

Lähde: Yleinen suomalainen ontologia 2019

Informaatio-operaatiot

Informaatio-operaatiossa on tarkoitus on koordinoidusti vaikuttaa siihen miten ihmiset ajattelevat ja toimivat, tai korruptoida julkista keskustelua strategisen tavoitteen saavuttamiseksi.

Informaatio-operaatiot

1. Harhauta ja petä kohdehenkilöä / -yhteisöä
- Käyttäydy kuin oikea media/näytä oikealta medialta

2. **Hyödynnä järjestelmän haavoittuvuuksia**
- Mielipiteen ilmaisunvapaus
- Avoin sosiaalinen media
- Luottamus tiedotusvälineisiin

3. **Riko sääntöjä**
- Valehtele
- Trollaus

Kognitiivinen sodankäynti

Kognitiivisessa sodankäynnissä tavoitteena on vaikuttaa siihen, miten vastustaja ajattelee ja toimii. Äärimmäisessä muodossaan tavoitteena on murskata ja hajottaa koko yhteiskunta niin, ettei sillä enää ole kollektiivista tahtoa vastustaa vastustajan aikeita.

Vastustaja haluaa alistaa yhteiskunta ilman suoraa voimaa tai pakkoa.

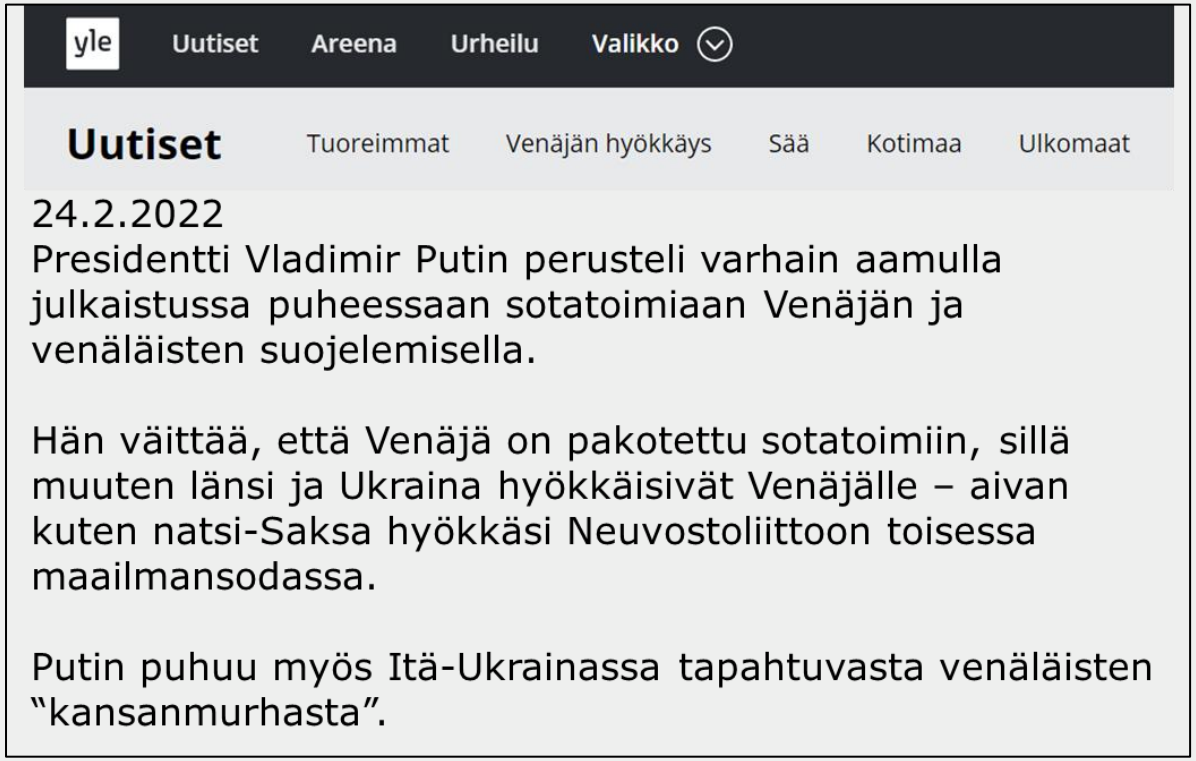
Keinoja:
- Dis-, mis- ja malinformaatiokampanjat
- Valeuutiset
- Tarkoitukselliset tietovuodot
- Some-kampanjat

Source: NATO review, Countering cognitive warfare: awareness and resilience, 20 May 2021

Strateginen kommunikaatio

Strateginen kommunikaatio on pitkän aikavälin kokonaisvaltaista toimintaa, jossa viranomaisyhteistyön, diplomatian, PR-työn ja informaatio-operaatioin edistetään kansallisia etuja.

Kansallinen narratiivi


yle Uutiset Areena Urheilu Valikko

Uutiset Tuoreimmat Venäjän hyökkäys Sää Kotimaa Ulkomaat

24.2.2022
Presidentti Vladimir Putin perusteli varhain aamulla julkaistussa puheessaan sotatoimiaan Venäjän ja venäläisten suojelemisella.

Hän väittää, että Venäjä on pakotettu sotatoimiin, sillä muuten länsi ja Ukraina hyökkäisivät Venäjälle – aivan kuten natsi-Saksa hyökkäsi Neuvostoliittoon toisessa maailmansodassa.

Putin puhuu myös Itä-Ukrainassa tapahtuvasta venäläisten "kansanmurhasta".

Informaatiovaikuttamista leimaa moniselitteisyys

Mikä osa vaikuttamisesta kuuluu tai ei kuulu yhteiskunnalliseen keskusteluun.

Poliittisten keskustelujen luonteeseen kuuluvat tunteet, kärjistykset ja kärjekkäätkin mielipiteet.

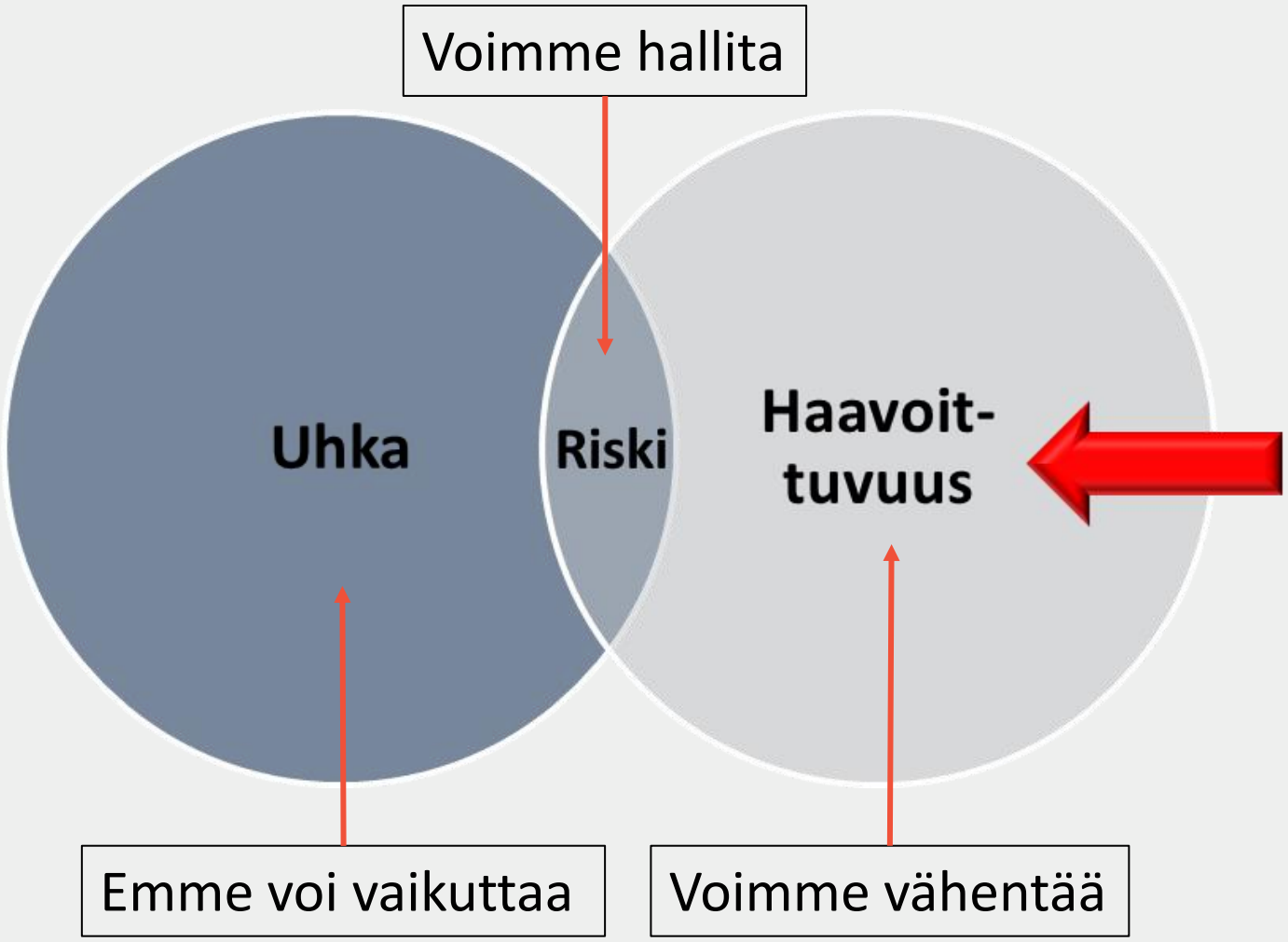
Demokratia perustuu avoimeen ja vapaaseen keskusteluun.

Mutta keskustelua on vaikea käydä rakentavasti, jos joku toimija esittää harhaanjohtavaa informaatiota tarkoituksenaan häiritä ja ohjata keskustelua.

Ihmisillä on oikeus mielipiteeseensä ja sen esille tuomiseen tai sen puolesta kampanjointiin.

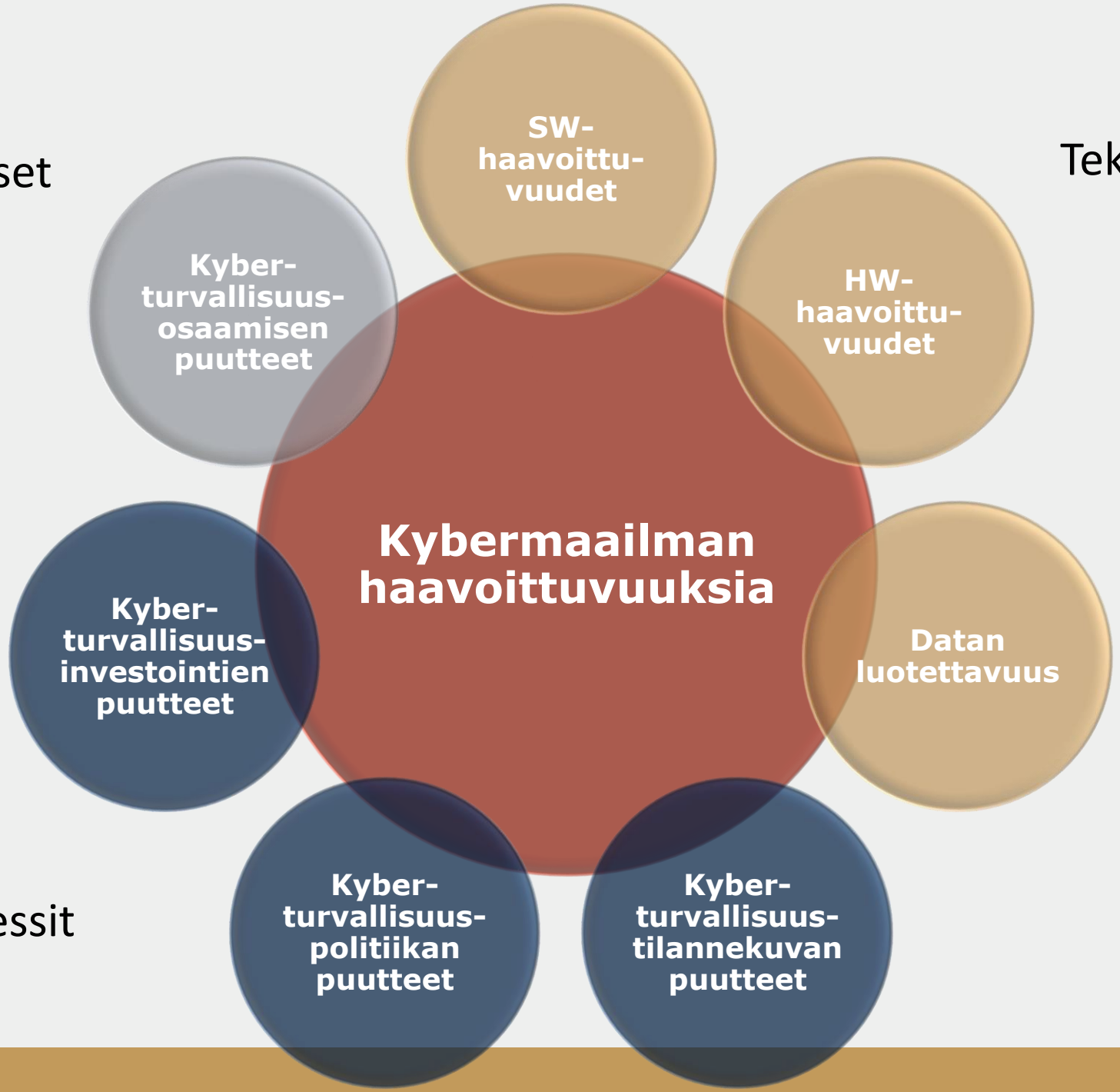
Esityksen sisältö

Uhka + haavoittuvuus = riski



Ihmiset

Teknologia



Prosessit

Kybermaailman haavoittuvuuksia

SW-haavoittuvuuksia

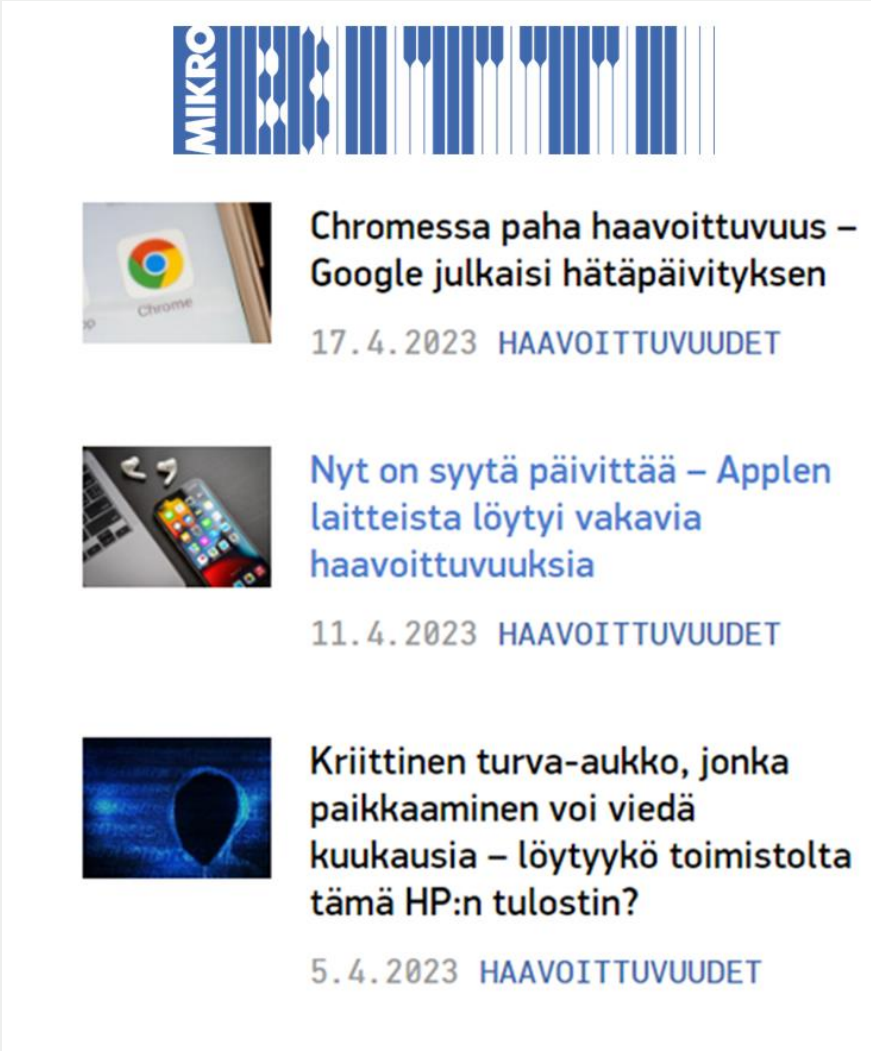
Ohjelman haavoittuvuus on virhe ohjelman koodaamisessa, konfiguroinnissa tai hallinnoinnissa.

Ohjelma voi olla algoritmi, sovellus, käyttöjärjestelmä, selain…

Hakkerit käyttävät haavoittuvuuksia ohjelmistohyökkäyksissä pakottaakseen järjestelmät antamaan heille pääsyn luvattomaan dataan, haitallisen koodin suorittamiseen, etähallinnan hankkimiseen tai saamaan järjestelmä levittämään tartuntaa.

SW-haavoittuvuuksia

Carnegie Mellon yliopiston CyLab Sustainable Computing Consortium on arvioinut, että ”kaupallisessa ohjelmistossa on 20-30 koodivirhettä jokaista 1000 koodiriviä kohden.



MIKRO

KIRJAUDU HAE SIVUSTOLTA

UUSIMMAT | TESTIT | NEUVOT | KESKUSTELU | BLOGIT | UUTISKIRJE | INFO

Venäläiset hakkerit varastelevat Naton sähköposteja – syy on vähän nolo

8.4.2023 20:01

Hidas haavoittuvuuksien paikkaaminen vaivaa korkea-arvoisiakin toimijoita.

Venäläinen hakkeriryhmä, joka tunnetaan myös nimellä **Winter Vivern**, on aktiivisesti käyttänyt hyväkseen Zimbra-sähköpostiohjelmiston haavoittuvuutta varastaakseen virallisia sähköposteja Naton virkailijoilta, hallituksilta, asevoimien edustajilta ja diplomaateilta.

SW-haavoittuvuuksia

ILTA-SANOMAT TUOREIMMAT LUETUIMMAT SÄÄ Kirjaudu Hae Valikko

ETUSIVU UUTISET VIIHDE URHEILU ME NAISET TALOUS AUTOT HYVÄ OLO DIGI RUOKALA ASUMINEN

TIETOTURVA

Haittaohjelma päätyi huippu-suosittuihin Android-sovelluksiin – ladattiin yli 100 miljoonaa kertaa

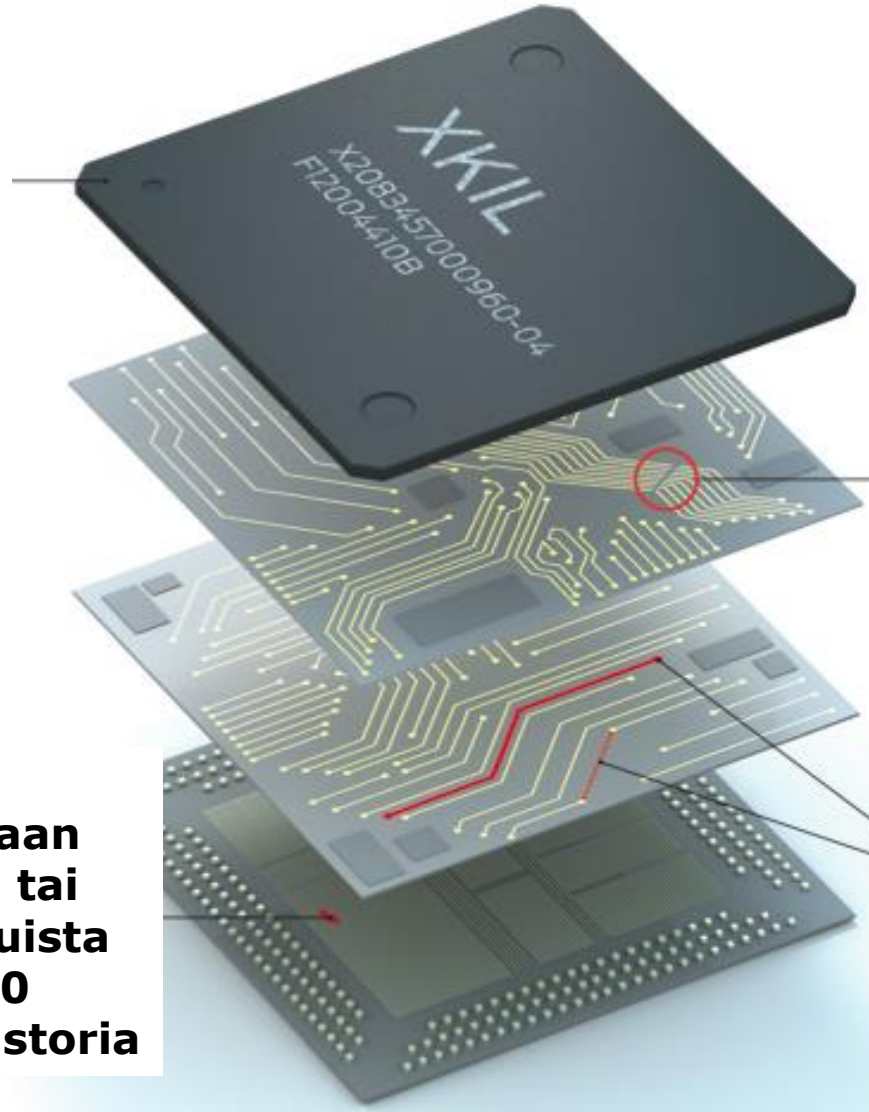
60 Android-sovellusta käytti tietämättään vaarallista ohjelmiston osaa Etelä-Koreassa ja muualla.

JAA KOMMENTOI

GOOGLE PLAY -sovelluskauppa tarjosi yli 60 Android-sovellusta, joissa oli mukana ulkopuolisen tahon haitallinen ohjelmakirjasto eli useiden sovellusten jakama ohjelmakomponentti. Tietoturvayhtiö McAfee antoi sille nimeksi Goldoson. Se kerää tietoa puhelimeen asennetuista sovelluksista, wifi- ja bluetooth-laitteista ja käyttäjän gps-sijainnista.

HW-haavoittuvuuksia

Kuumennus-käsittely lyhentää sirun käyttöikää 15 vuodesta 6 kuukauteen.



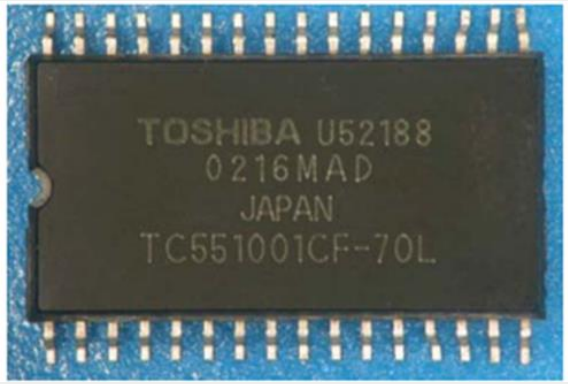
Käsittelemällä piirikytkentöjä voidaan heikentää sirun kestävyyttä kuormitus-tilanteessa

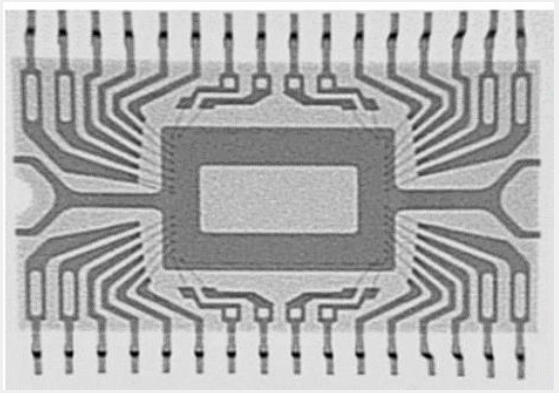
Lisäämällä transistoreita voidaan tehdä takaportteja tai tappokytkimiä. Siruista on löydetty yli 1000 ylimääräistä transistoria

Lisäämällä ja muuttamalla piirikytkentöjä, voidaan tehdä uusia ei-haluttuja toiminnallisuuksia.

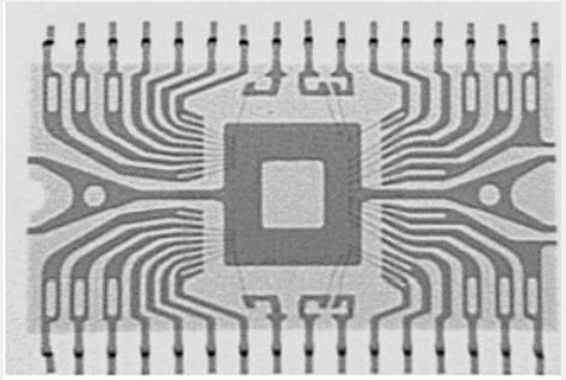
Source : Thehuntforthekillswitch.http://www.spectrum.ieee.org/semiconductors/ design/the-hunt-for-the-kill-switch.

HW-haavoittuvuuksia
Component corruption





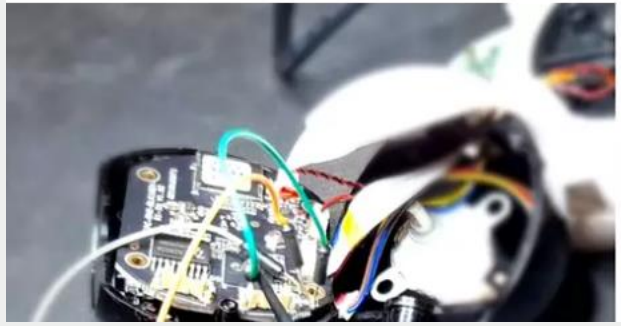
Röntgenkuvaus



Suomessa myyty 1 300 vaarallisen takaportin sisältänyttä netti-kameraa – myynnissä myös Prismoissa

Laite on nyt vedetty pois Prismoista, mutta sitä on vielä myynnissä pienemmissä kaupoissa.

JAA KOMMENTIT



Datan luotettavuus

“Cyber Armageddon is less likely than cyber operations that will change or manipulate data.”

10.9.2015

The directors of the FBI, James Comey, CIA, John Brennan, National Intelligence, James Clapper, NSA, Michael Rogers, and Defense Intelligence Agency, Lieutenant General Vincent Stewart.

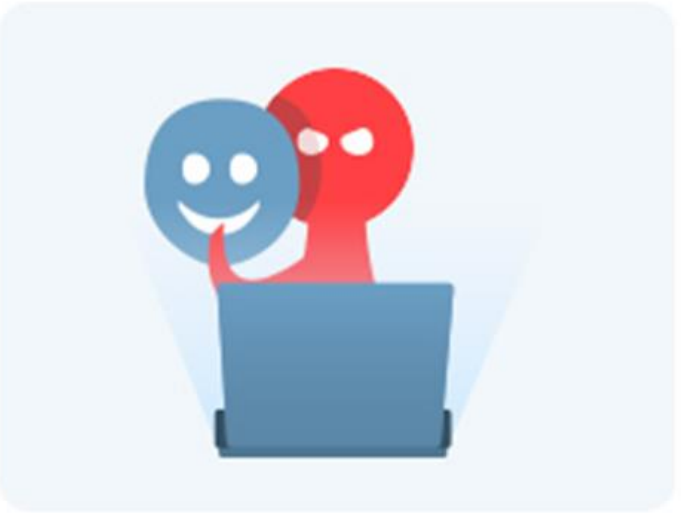
Sisäpiiriuhat

Pahantahtoinen sisäpiiriläinen

Käyttää mahdollisuutta päästä käsiksi sensitiiviseen tietoon ja tuottaa vahinkoa yritykselle.

Huolimaton sisäpiiriläinen

Altistaa organisaation toimimalla turvallisuusohjeiden vastaisesti



Hakkeroitu sisäpiiriläinen

Hänen käyttäjätilinsä on murrettu, vaikka hän on toiminut oikein.

LastPassin karmea tietomurto olisi voitu estää asentamalla kolme vuotta vanha päivitys – ”korjaava versio julkaistiin jo noin 75 versiota sitten”

Petteri Uusitalo6.3.202309:49|päivitetty6.3.202309:49TIETOMURROTHAAVOITTUVUUDETTIETOTURVASALASANANHALLINTA

Salasanapalvelun tietomurto tehtiin siten kuten tietomurrot yleensä: ihmisen huolimattomuutta hyödyntämällä.

Salasanapalvelu LastPass joutui viime vuoden puolella useamman katastrofaalisen tietomurron kohteeksi. Helmikuussa se lopulta kertoi, miten murroista jälkimmäinen oli tapahtunut: merkittävässä roolissa olevan työntekijän salasana oli varastettu tämän kotitietokoneelta hyödyntämällä mediaserveriohjelmisto Plexissä ollutta tietoturva-aukkoa.

Yhdysvallat

The New York Times: Yhdysvaltojen tietovuotaja paljasti asiakirjoja jo luultua aiemmin ja paljon laajemmalle yleisölle

Sanomalehden mukaan Yhdysvalloissa pidätetty tietovuotaja näyttää levittäneen salaisia tietoja jo helmikuussa 2022, vain 48 tuntia Venäjän hyökkäyssodan alkamisen jälkeen.

Mielipiteenmuodostus

MEDIAJÄRJESTELMÄN HAAVOITTUVUUDET
Väärennetyt viestit, manipuloidut kuvat, klikkien kalastelujahti, algoritmit ja sosiaalisessa mediassa toimivat botit.

HAAVOITTUVUUDET MIELIPITEENMUODOSTUKSESSA
Kuulumme erilaisiin sosiaalisiin ja informaatiokupliin, joissa vahvistuu samanmielisyys, mikä saattaa vahvistaa ennakkoluuloja ja edelleen vastakkainasettelua.
Tätä väärennetyt sosiaalisen median tilit ja trollit lisäävät entisestään.

KOGNITIIVISET HAAVOITTUVUUDET
Tietotulvan keskellä emme pysty erottamaan oikeaa tietoa väärästä.
Some-alustat keräävät tietoa ja muodostavat meistä profiileita.
Näitä tietoja pystytään hyödyntämään. Järjestelmät ymmärtävät meitä paremmin kuin mitä me itse teemme.

Lähde: VNK, Informaatiovaikuttamiseen vastaaminen -Opas viestijöille, Valtioneuvoston kanslian julkaisuja 2019:11

Kybermaailmassa on 0-luottamus

Ihmisten luotettavuus
Autentikointi- ja auktorisointihaasteet

Component corruption
Kill Switch

Koodivirheet, bugit
Rogue applications
Back doors
Kill Switch

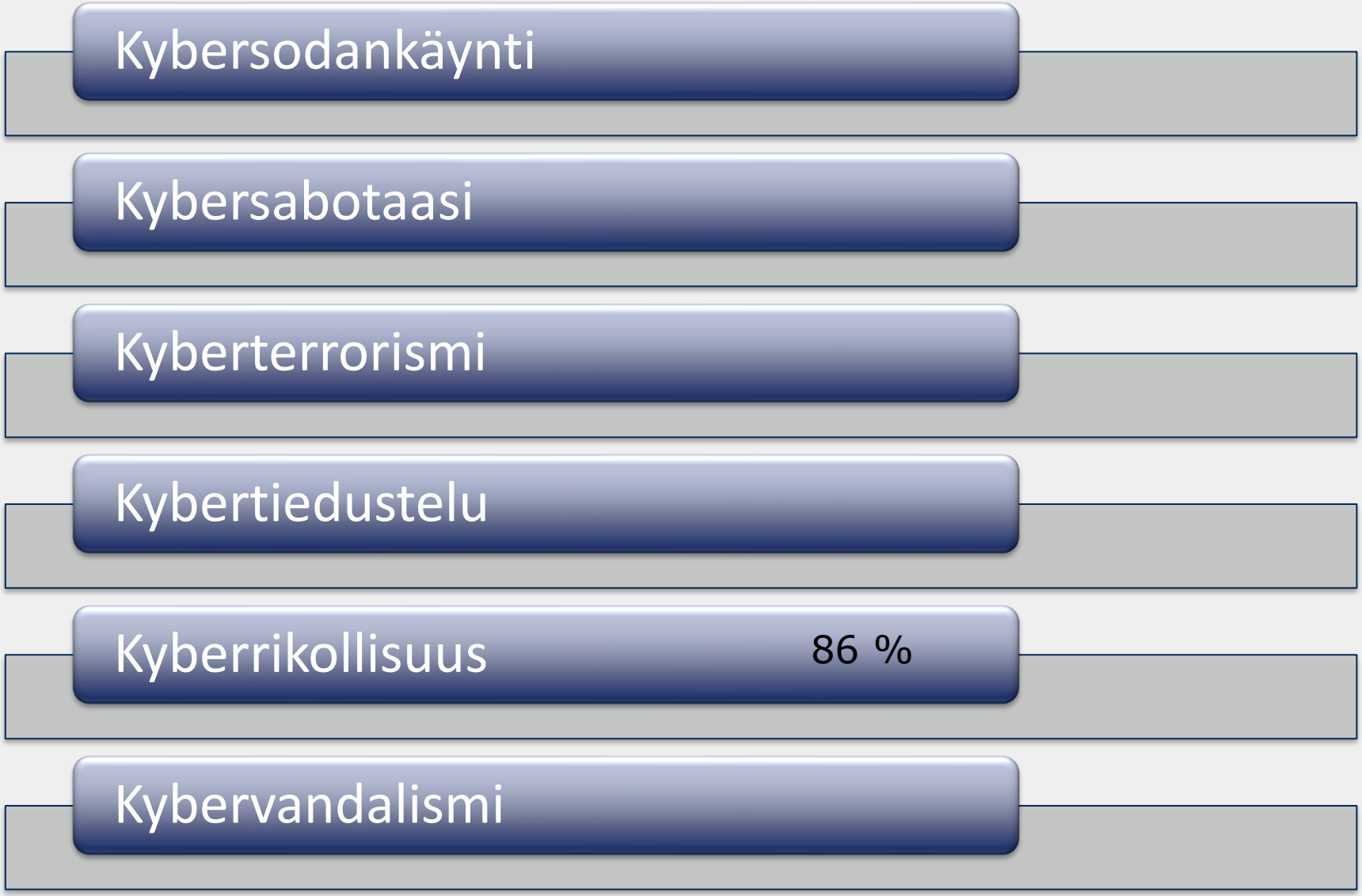
SCADA-, ICS-, IT-, OT-järjestelmien haavoittuvuudet

Datan manipulointi

Huono verkkokonfiguraatio
Verkon ”valvonta”

Esityksen sisältö

Kyberuhkamalli

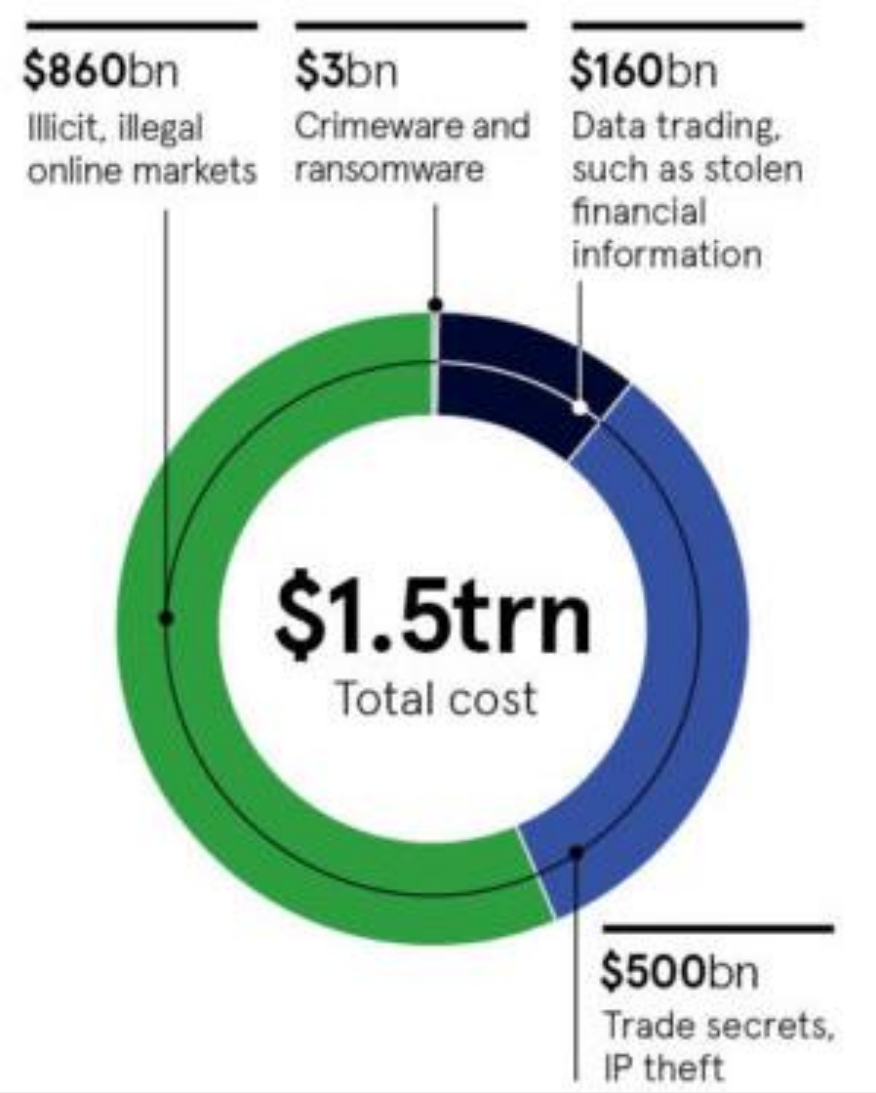


Motivaatio ratkaisee

Kyberrikollisuus

1. Perinteiset rikollisuuden muodot.
2. Laittoman sisällön julkaiseminen sähköisissä viestimissä.
3. Rikokset, joita esiintyy ainoastaan sähköisissä verkoissa.

Kyberrikollisuuden liikevaihto yli 1,5 biljoonaa dollaria joka vuosi



Kyberrikollisuuden liikevaihto:

- Laiton verkkokauppa $860 miljardia
- Liikesalaisuuksien ja IPR:n varkaudet $500 miljardia
- Varastetun datan myynti $160 miljardia
- Crime-ware/CaaS $1,6 miljardia
- Lunnashaittaohjelma $1 miljardi

Suurimmat lunnaat Ransomware-hyökkäyksestä: $40 miljoonaa

Kyberturvallisuus-vakuuttaminen $ 7,5 miljardia, vuonna 2030 $ 28 miljardia

Source: Re-Hashed: 2018 Cybercrime Statistics: A closer look at the "Web of Profit", September 27, 2018

Kyberrikos palveluna

Tuotteita
- Haittaohjelmia
- Exploitteja
- Henkilötietoja

Hacking email
from
$40

Hacking website
from
$150

Targeted attack
from
$4,500

DDoS attack
from
$50
a day

Infecting with ransomware Trojan (1,000 nodes)
from
$750

Stealing from ATM
from
$1,500

Infecting with Trojan for mining (1,000 nodes)
from
$300

Stealing payment data
from
$270

Dataa myynnissä:
- Käyttäjätunnuksia
- Salasanoja
- Luottokorttitietoja
- Yritystietoja

Keyword found: Hacking tools
Location: https://crackingitaly.to/profile/69996-adiss/
Time: 8 hours ago 28/09/2021 8:59:25

Domain: crackingitaly.to EXCLUDE THIS DOMAIN
TO BOOKMARKS:
Title: Adiss - CrackingItaly

TXT COPY

```
... * Downloads
* Downloads
* BruteForces Tools
* Cracking Tools
* Wordlist / Combo
* More
* More

!(https://crackingitaly.to/logo-ci-ob.png)

## OpenBu...

...
* #### Downloads

* Back
* BruteForces Tools
* Cracking Tools
* Wordlist / Combo

x

* Create New...
* Status
* Topic
* Donate
* Post New Video
...
```

cybernews News Editorial Security Privacy Crypto Cloud Resources Tools Reviews Follow

If you purchase via links on our site, we may receive affiliate commissions.

Home » Security

RockYou2021: largest password compilation of all time leaked online with 8.4 billion entries

by Edvardas Mikalauskas 07 June 2021 34

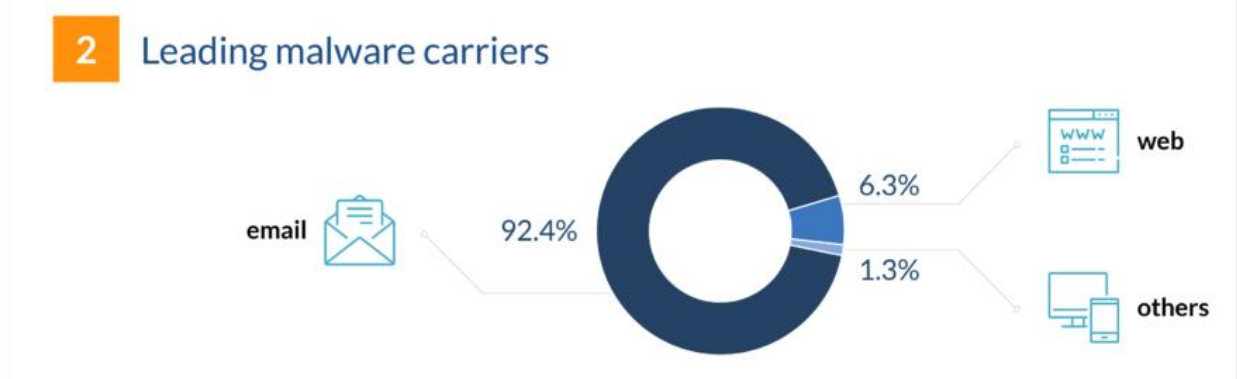
Source: Rob Freeman, Cyber attack software products for sale, 17th January 2019

Sähköposti on edelleen verkkorikollisten suosikkikanava

Sähköposti on eniten käytetty ja kustannustehokas sekä helppo haittaohjelmien jakelukanava.

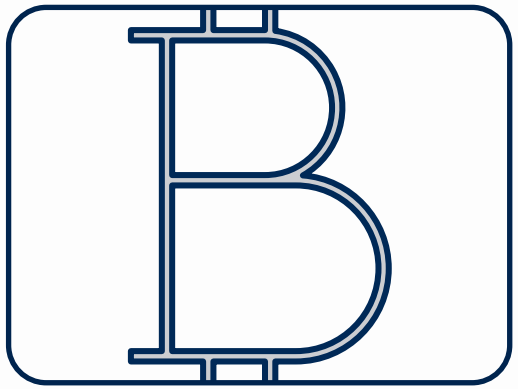
Sen avulla toteutetaan tietojenkalastelua, ja haittaohjelmien asentamista (takaovet, tiedostovarkaudet ja tuhoaminen).

Tietoja voi käyttää myöhemmin mm. kohdennettuihin hyökkäyksiin, tietomurtoihin, identiteettivarkauksiin, erilaisiin huijauksiin ja sabotaasioperaatioihin.

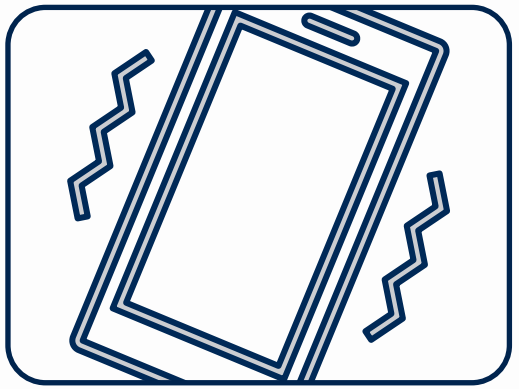


Kyberrikollisten digipalvelualusta

TOR-verkko, 2004 anonyymiin viestintään.



Kryptovaluutta (Bitcoin, 2008) anonyymiin maksuliiken-teeseen.



Salattu mobiiliviestintä (Wickr, 2012) anonyymiin keskusteluun.

Anonymiteetti antaa kyberrikollisille erinomaisen suojan

Lunnashaittaohjelma lamautti sairaalan

400 sairaalaa ja hoitolaitosta

Syyskuu 2020:

Lunnashaittaohjelmahyökkäys lamautti koko sairaalaketjun IT-järjestelmän:

- Puhelinjärjestelmä ei toiminut,
- Tietojärjestelmät eivät toimineet,
- Potilastiedot kirjattiin paperilla ja kynällä,
- Potilaita ohjattiin muihin sairaaloihin,
- Testitulosten saaminen viivästyi.

Palautus kesti 3 viikkoa
Tulon menetykset $42.1 miljoonaa
Kokonaistappio $67 miljoonaa

President Rodrigo Chaves says Costa Rica is at war with Conti hackers

18 May

Costa Rican presidentti sanoo, että hänen maansa on "sodassa", koska kyberrikolliset aiheuttavat suuria häiriöitä useiden ministeriöiden IT-järjestelmiin.

Rodrigo Chaves sanoi, että hakkerit soluttautuivat 27 valtion laitokseen, mukaan lukien kunnat ja valtion ylläpitämät laitokset.

Venäläinen Conti-kartelli vaatii 20 milj. USD lunnaita.

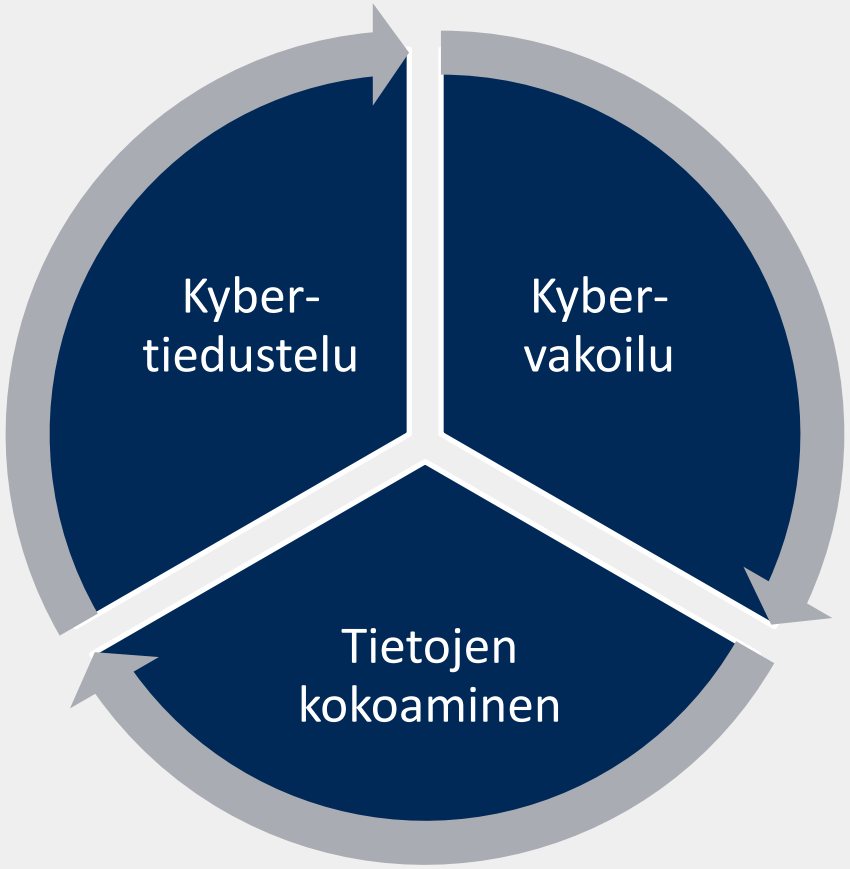
Vaikutuksia:

- Valtion maksupalvelu ei toimi
- Valtion tilinpito ei onnistu
- Verotus- ja tullaus ei toimi

Kybertiedustelu-vakoilu-tiedon kokoaminen

Turvallisuuspalveluiden lakisääteistä toimintaa.

Tähän liittyy myös kybervastatiedustelu.



Valtiollisten tai muiden toimijoiden toteuttamaa toimintaa sekä proxien käyttöä.

Kaikki digitaalisia palveluita tuottavat yritykset keräävät erilaista asiakastietoa.

Avoin WLAN

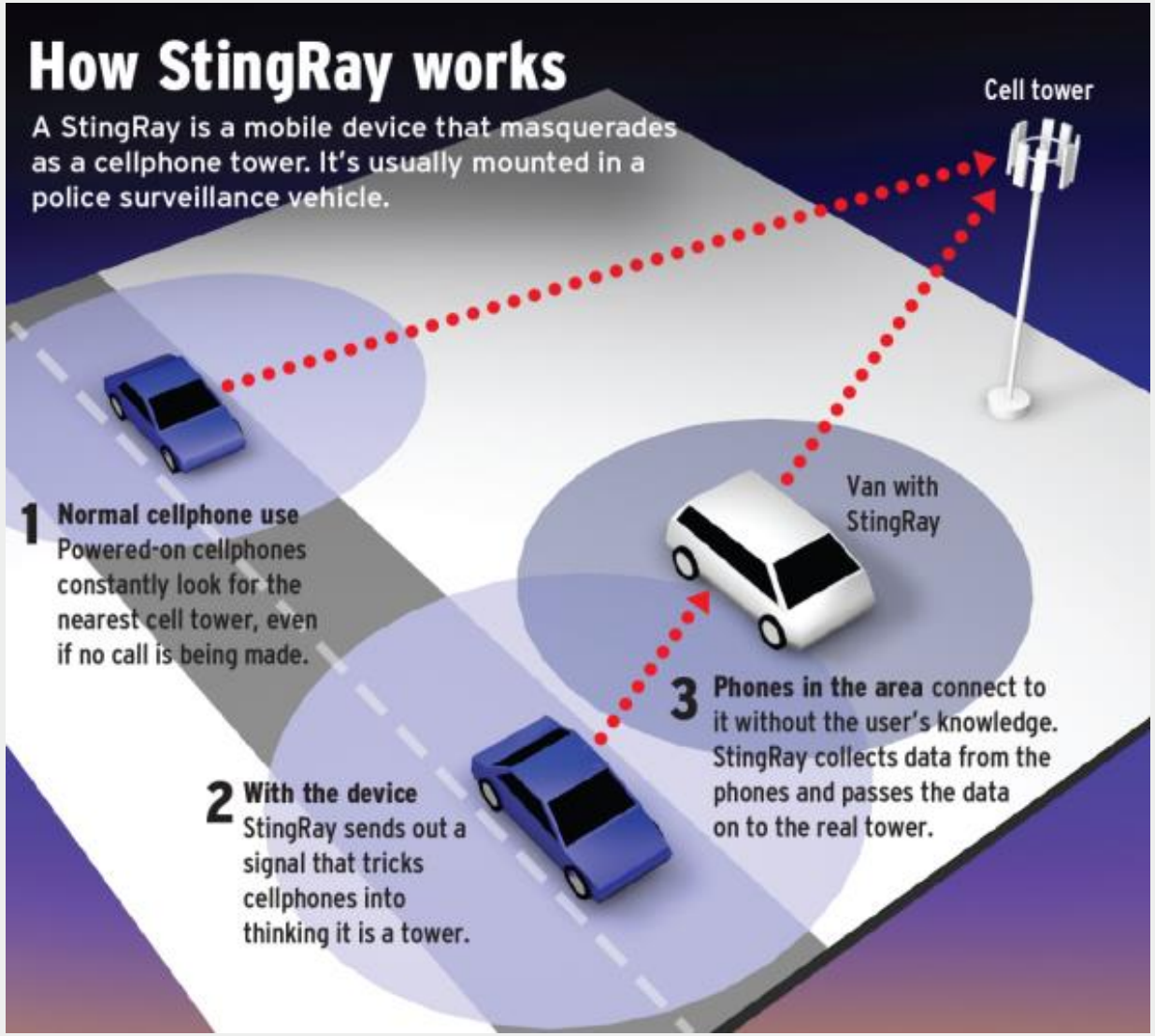
11.1.2015 Sälen

Ruotsin piraattipuolueen nuortenjärjestön puheenjohtaja **Gustav Nipe** loi puolustus- ja turvallisuuskonferenssiin wlan-verkon nimeltä Öppen Gäst.

Moni konferenssivieras erehtyi kirjautumaan huijausverkkoon. Nipe onnistui seuraamaan arviolta sadan poliitikon, toimittajan ja tietoturva-asiantuntijan netin käyttöä. Hän pystyi seuraamaan, millä sivuilla verkon käyttäjät vierailivat ja myös lukemaan heidän sähköposti- ja tekstiviestejään.

StingRay

StingRay-laite teeskentelee olevansa mobiilitukiasema ja sieppaa puhelinten tunnistekoodeja, seuraa puhelinten sijaintia ja jopa kaappaa puheluja ja tekstiviestejä.



Matkapuhelin tiedustelukohteena

SS7-protokollaa väärinkäyttämällä on mahdollista:

- Käyttäjän sijainnin selvittäminen ja seuraaminen
- Puheluiden salakuuntelu ja nauhoittaminen
- Radioliikenteessä käytetyn salauksen purkaminen
- Liittymän irti kytkeminen matkapuhelinverkosta eli viestinnän estäminen ja
- Liittymän laskutuksen manipuloiminen petoksellisesti.

(Signalling System 7)

Lähde: Kyberturvallisuuskeskus, 2014

Pegasus-vakoiluohjelma matkapuhelimessa

NSO Groupin Pegasus on haittaohjelma, jonka avulla infektoituneessa matkapuhelimessa voidaan mm. lukea viestejä, seurata puheluita, kerätä salasanoja, seurata sijaintia ja aktivoida mikrofoneja.

Keskiviikko 31.5.2023 Helga, Helka

TELKKU KOTIKOKKI ETUA KATTOKORKO NÄKÖISLEHTI

ILTALEHTI Tampere 16°

TILAA PLUS KIRJAUDU

Etusivu Uutiset Urheilu Viihde Plus Sää IL-TV Autot Terveys Hyvä olo Tyyli.com Asuminen Perhe Pippuri.fi Matkailu Raha Digi

Digiuutiset Testit Pelit ja esports Tietoturva Hintaopas

DIGI & TEKNIIKKA

DIGI & TEKNIIKKA | TIETOTURVA

Poista tämä sovellus puhelimestasi heti – Päivityksen sisään oli ujuttautunut haittaohjelma

Suosittu näytöntallennus-sovellus kerää käyttäjästään tietoja ja lähettää ne haittaohjelman ylläpitäjälle.

Slovakialainen kyberturvallisuusyhtiö ESET varoittaa iRecorder - Screen recorder näytöntallennus-sovelluksesta. Sovellus on ollut saatavilla Android-käyttäjille.

ESET:in mukaan kyseinen sovellus ajaa käyttäjän huomaamatta haittaohjelmaa normaalin käytön taustalla. Sovellus nauhoittaa minuutin mittaisen äänipätkän 15 minuutin välein. Lisäksi sovellus kerää tietoja puhelimen tiedostoista sekä verkkoselaimesta.

Sovellus lähettää kerätyt tiedot haittaohjelman ylläpitäjälle.

Kiinan kybertiedustelu

Kiinan vuoden 2017 kansallinen tiedustelulaki vaatii kaikkia yrityksiä “tukemaan, tarjoamaan apua, ja tekemään yhteistyötä kansallisessa tiedustelutoiminnassa ja huolehtimaan hallussaan olevan kansallisen tiedustelutiedon turvallisuudesta.

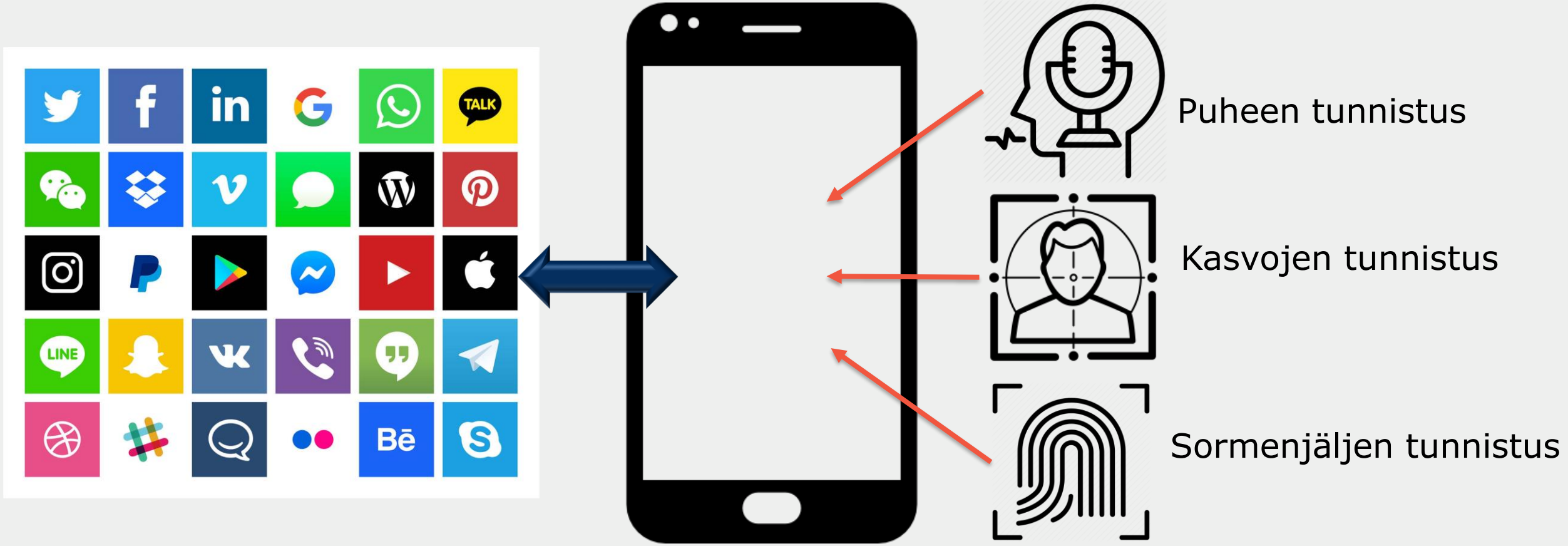
Valtion on suojeltava henkilöitä ja organisaatioita, jotka tukevat, tekevät yhteistyötä ja toimivat yhteistyössä kansallisessa tiedustelutoiminnassa.”

Source: The National People's Congress passed the law on 27 June 2017

Kansalainen ja tiedon kokoaminen

Erilaisten digitaalisten palveluiden käyttäjinä olemme antaneet luvan tietojen kokoamiseen, jakamiseen ja käyttämiseen.

Paras tiedustelukohde ikinä



Paikannuspalvelu

Google Mapsissa ”on yli 220 maata ja aluetta sekä satoja miljoonia yrityksiä ja paikkoja. Voit hyödyntää reaaliaikaista GPS-navigointia sekä tietoja liikennetilanteesta ja julkisesta liikenteestä sekä tutkia paikallisia alueita ja selvittää, missä kannattaa käydä syömässä, juomassa tai vierailulla – olitpa itse missä päin maailmaa tahansa.”

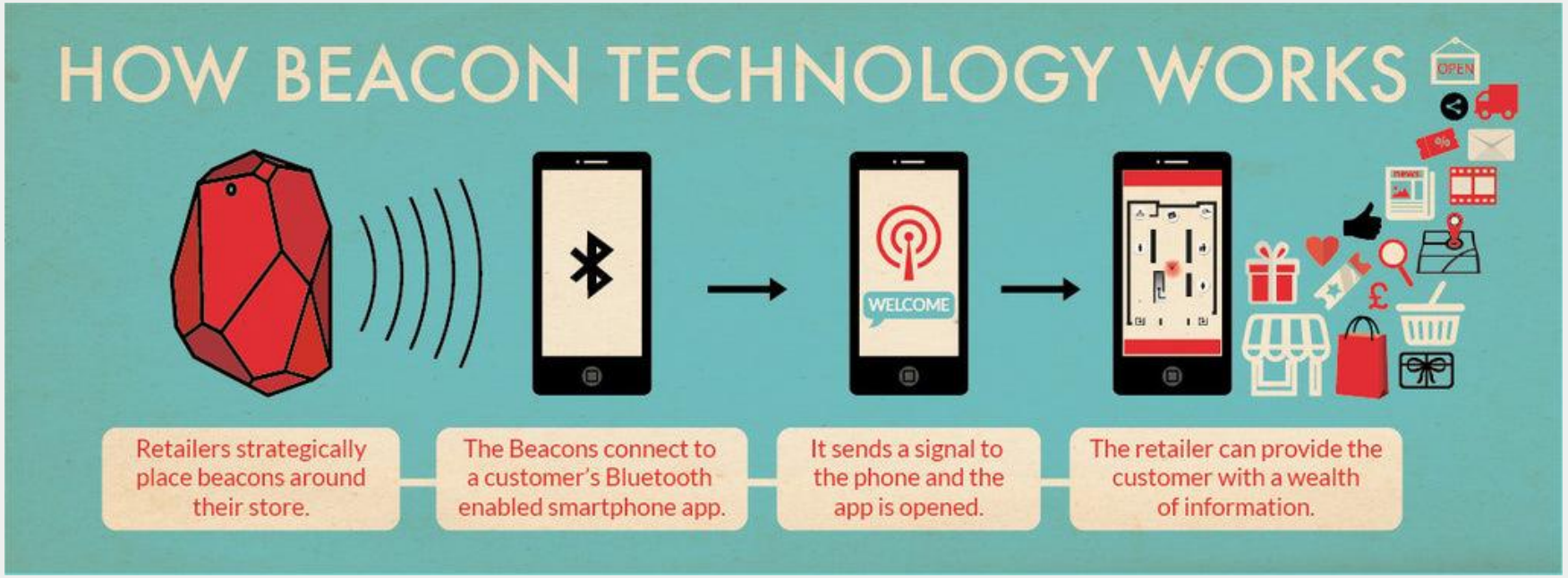
Sinun ja Googlen välinen sopimussuhde

Yleisesti ottaen annamme sinulle luvan käyttää palveluitamme, jos suostut noudattamaan näitä ehtoja, jotka ovat sidoksissa Googlen liiketoimintoihin ja tapoihin ansaita tuloja

Tämän käyttöoikeuden nojalla Google saa:

- ylläpitää, jäljentää, jaella, välittää ja käyttää sisältöäsi,
- julkaista sisältöäsi tai esittää tai näyttää sitä julkisesti,
- muokata sisältöäsi esimerkiksi muotoilemalla sitä uudelleen tai kääntämällä sitä,
- alilisensoida nämä oikeudet:
  - muille käyttäjille,
  - sopimuskumppaneille,

Älypuhelimesta seurantalaite



Tietoja kuluttajien sijainnista keräämiä majakoita on maailmassa miljardeja. Niitä asennetaan kaikkialle, missä ihmiset viettävät aikaa: ravintoloihin, kauppoihin, urheilustadioneille, kenkäosastolle tai hotellin aulaan, missä ne sulautuvat sisustukseen. Niitä on valvontakameroissa, lampuissa, kattopaneeleissa.

Majakka vastaanottaa tunnisteen, kun puhelimesi saapuu kantaman alueelle. Algoritmi taas tietää, kenestä on kyse.

Kun lataat jonkin sovelluksen, joudut hyväksymään käyttöehdot ja sallit paikantamisen.

Estääkö päästä-päähän salaus?

”Monet viestintäohjelmat salaavat viestit vain sinun ja heidän palvelimiensa välillä, mutta WhatsAppin täysi salaus varmistaa, että vain sinä ja henkilö, jonka kanssa keskustelet, voi lukea viestejä - ei kukaan muu. Ei edes WhatsAppin henkilökunta.”

Saksalaiset tutkija kertovat useista puutteista salausapplikaatioissa kuten WhatsApp, Signal, ja Threema. Turvallisuus ryhmäkeskusteluissa voi vaarantua.

Kasvojen tunnistuksesta tunteiden tunnistukseen

Automaattinen kasvojen tunnistus ihmismassojen skannaamisen.

Facebook käyttää palvelussaan automaattista kasvojen tunnistusta.

Windows 10 sisältää Windows Hello –palvelun.

Kasvojen tunnistusta voidaan käyttää myös yksinkertaisten perusilmeiden tunnistamiseen, millä pyritään yhdessä tekoälyn kanssa tunteiden tulkintaan.

Yksilön tunnistaminen

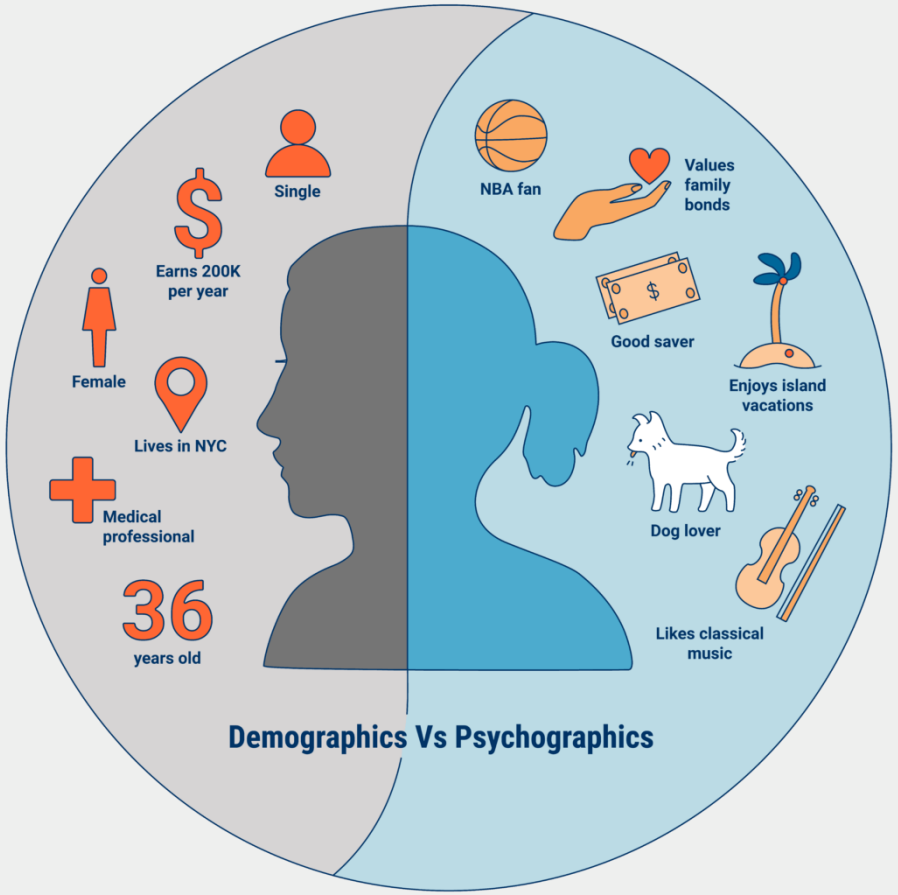
Persoonallisuuden tunnistaminen

Mikrokohdentaminen

Uusien markkinointiteknologioiden ylivoimainen ominaisuus on ollut tunnistaminen ja kohdistaminen.

Päätelaitteista, medioista, sisältö- ja julkaisualustoista ja -palveluista sekä tietoon, tiedon vaihtoon ja tiedon hyödyntämiseen perustuvasta yhteiskunnasta on tullut yksilökeskeistä.

Henkilötiedot analyysin kohteena: Psychographics



Tietolähteet

Evästeet, kanta-asiakasohjelmat, some-palvelut, julkiset rekisterit…

Arvot, asenteet, käyttäytyminen

Mikrokohdentaminen

- Kuluttajamainonta
- Sopimuksen vastainen käyttö

Psykologisia tietoja on sovellettu persoonallisuuden, arvojen, mielipiteiden, asenteiden, etujen ja elämäntapojen tutkimiseen.

Esityksen sisältö

Henkilökohtaisen kyberturvallisuuden pilarit

Datan suojaaminen

Henkilökohtaisten tietojen suojaaminen tietomurroilta ja tuhoutumiselta

Yksityisyyden suojaaminen

Henkilökohtaisten tietojen kontrollointi verkkopalveluissa ja niihin pääsyn hallinta

Laitteiden suojaaminen

Keinot päätelaitteiden suojaamiseksi luvattomalta tunkeutumiselta ja käytöltä

12 ohjetta henkilökohtaiseen kyberturvallisuuteen

1. Pyri ymmärtämään palvelun käyttöehdot.
2. Käytä kaikissa nettilaitteissa luotettavia suojausohjelmistoja ja hoida päivitykset.
3. Kaikki nettiin laitettu on siellä ikuisesti – mieti mitä sinne tallennat.
4. Käytä hyvää salasanaa (salasana/palvelu), äläkä tallenna sitä selaimeen.
5. Käytä kaksivaiheista tunnistusta aina, kun mahdollista.
6. Ole tarkkana kenen kanssa hoidat raha-asioita netissä.
7. Älä ole yhteydessä tuntemattomiin netissä.
8. Älä avaa epäilyttäviä posteja, erityisesti liitetiedostoja tai linkkejä.
9. Älä liitä laitteisiisi muiden lisälaitteita (USB-tikku, irtokovalevy, nettikamera yms.).
10. Käytä etätyöskentelyssä VPN-yhteyttä.
11. Toteuta toimiva varmuuskopiointijärjestely.
12. Mieti ensin – klikkaa sitten

Kiitos

www.jyu.fi/it