JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Kyberturvallisuusuhat ja informaatiovaikuttaminen kokonaisturvallisuusympäristössä

Tutkimusjohtaja, ST ev evp. Martti Lehto

10.10.2024

Esityksen sisältö

1. Digitaalinen kybermaailma
2. Kybermaailman haavoittuvuuksia
3. Kybermaailman uhkia
4. Informaatiovaikuttaminen
5. Johtopäätöksiä

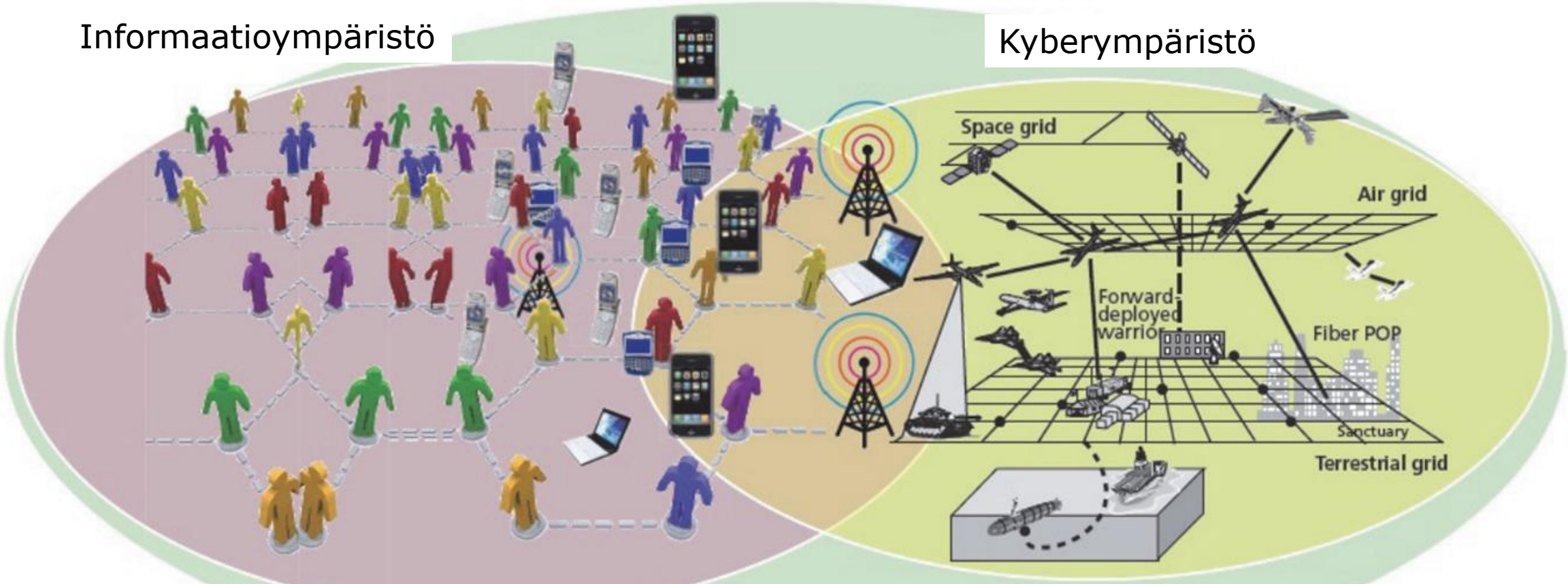
FBI chief says Chinese hackers have infiltrated critical US infrastructure

Volt Typhoon hacking campaign is waiting 'for just the right moment to deal a devastating blow', says Christopher Wray

Chinese government-linked hackers have burrowed into US critical infrastructure and are waiting "for just the right moment to deal a devastating blow"

FBI director, Christopher Wray, speaks during a House hearing in Washington DC on 11 April 2024.

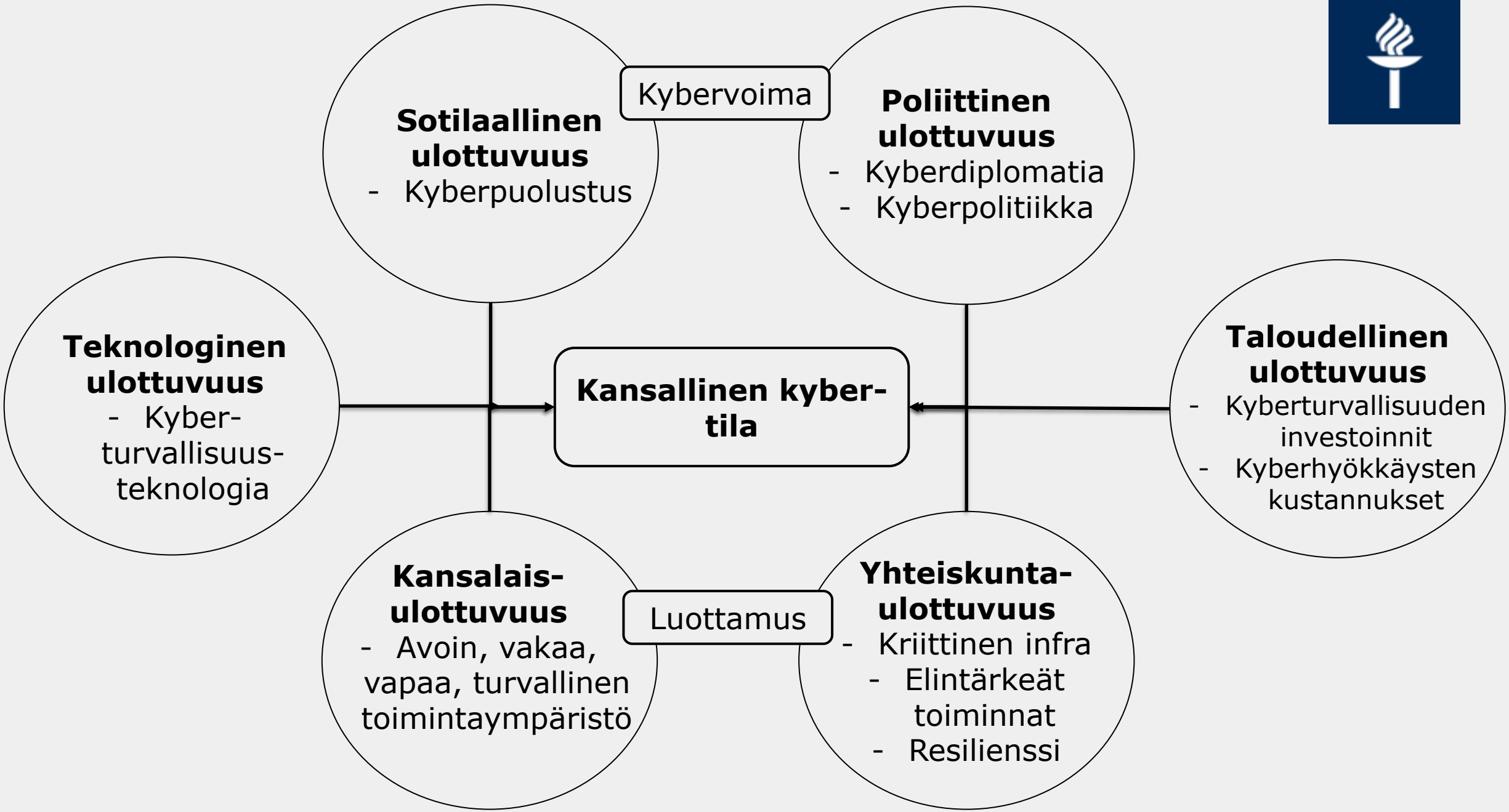
Kyberympäristö vs. Informaatioympäristö

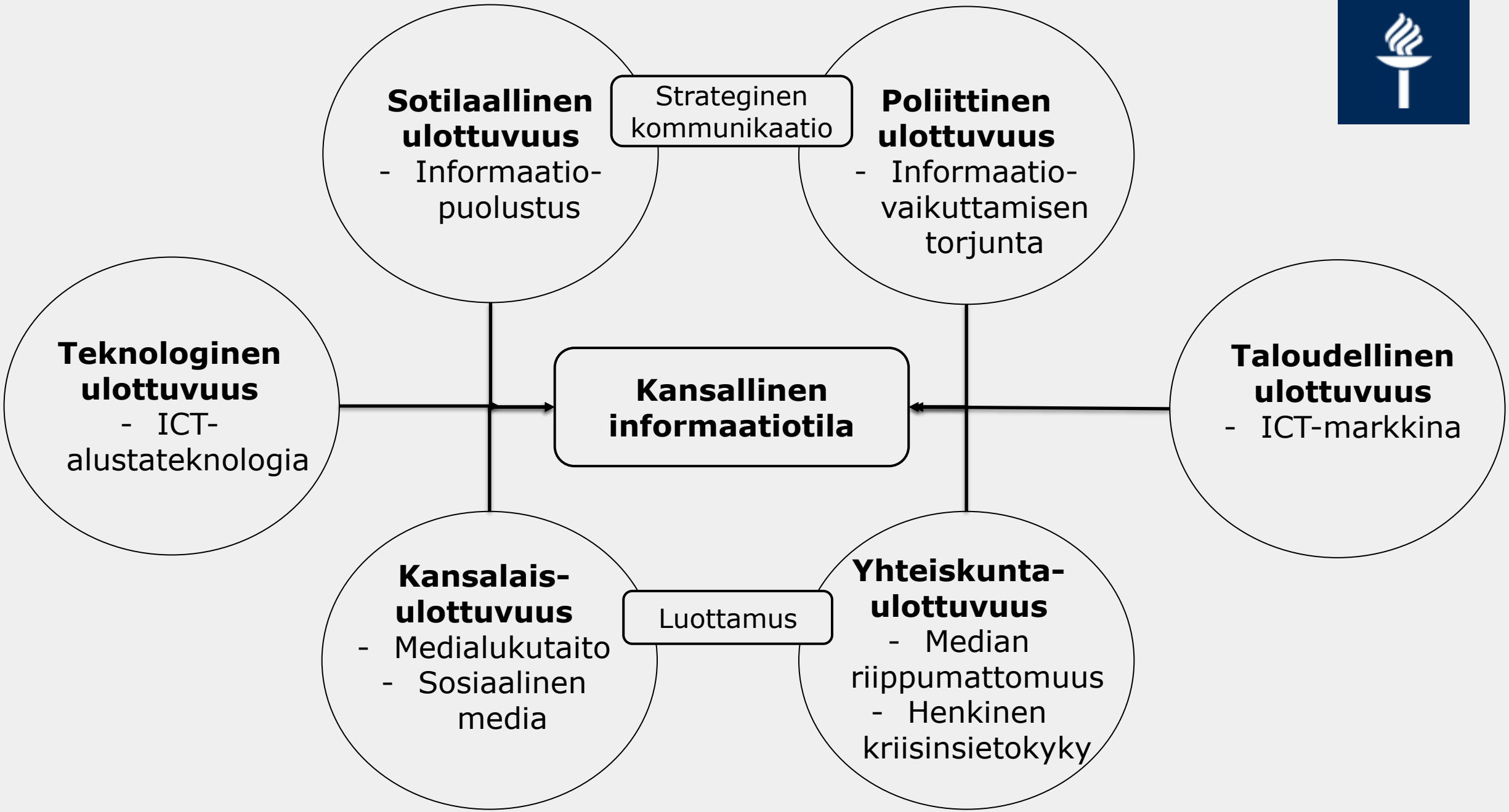


Informaatioympäristö on reaalinen ja virtuaalinen tila, jossa eri verkostoissa informaatiota vastaanotetaan, käsitellään ja välitetään

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
Teknologinen ulottuvuus
- Kyber-turvallisuus-teknologia
Kansallinen kyber-tila
Taloudellinen ulottuvuus
- Kyberturvallisuuden investoinnit
- Kyberhyökkäysten kustannukset
Kansalais-ulottuvuus
- Avoin, vakaa, vapaa, turvallinen toimintaympäristö
Luottamus
Yhteiskunta-ulottuvuus
- Kriittinen infra
- Elintärkeät toiminnat
- Resilienssi


Sotilaallinen ulottuvuus
- Informaatio-puolustus
Strateginen kommunikaatio
Poliittinen ulottuvuus
- Informaatio-vaikuttamisen torjunta
Teknologinen ulottuvuus
- ICT-alustateknologia
Kansallinen informaatiotila
Taloudellinen ulottuvuus
- ICT-markkina
Kansalais-ulottuvuus
- Medialukutaito
- Sosiaalinen media
Luottamus
Yhteiskunta-ulottuvuus
- Median riippumattomuus
- Henkinen kriisinsietokyky

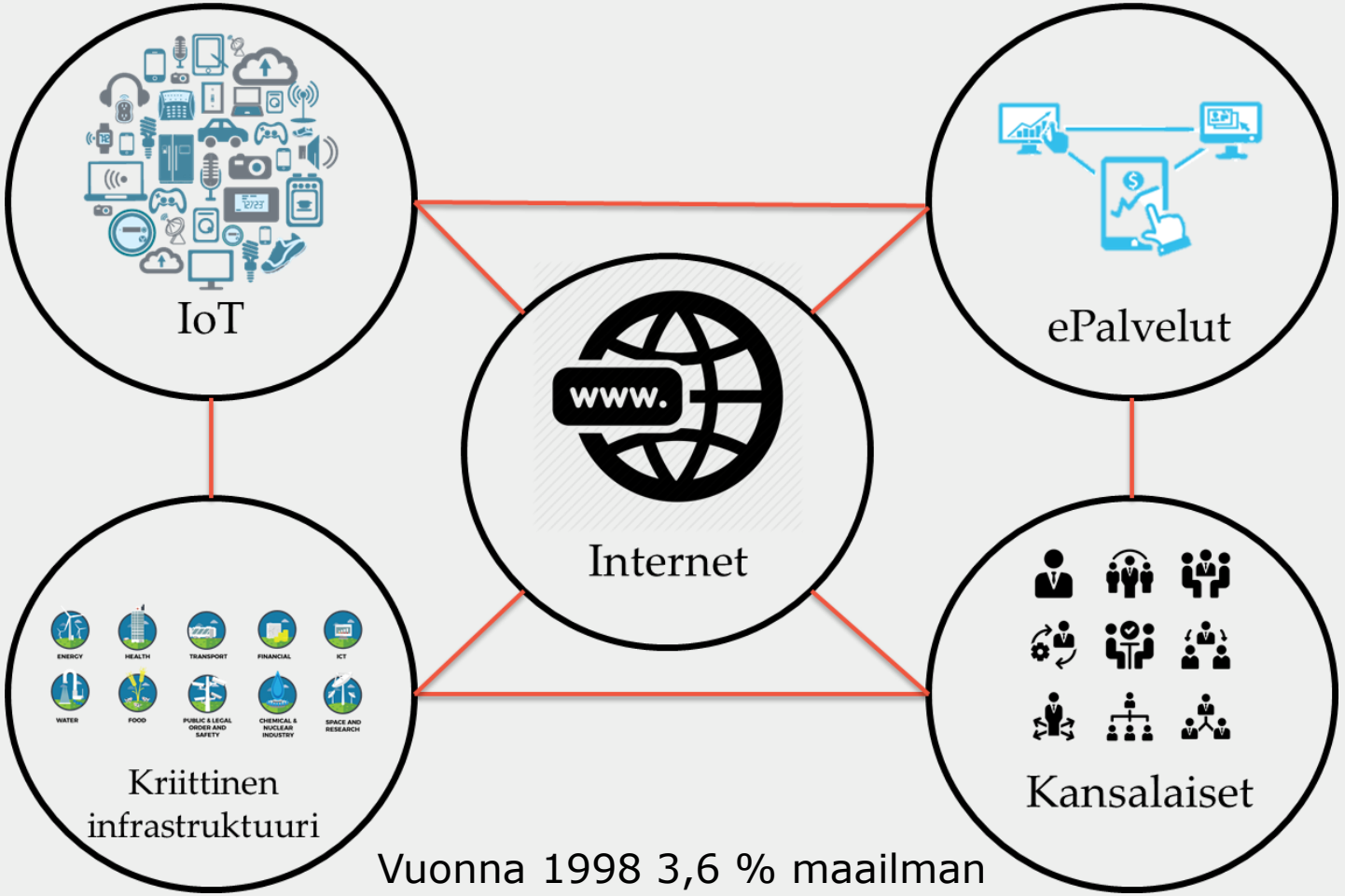
Digitaalinen kybermaailma 2024

Maailmassa 50 miljardia verkkoon kytkettyä laitetta. Vuonna 2030 yli 125 miljardia.

Matkapuhelinten käyttäjiä maailmassa on yli 7,4 miljardia (92 %).

Älypuhelinten käyttäjiä yli 7 miljardia (88 %).

Vuonna 2023 ladattiin noin 257 miljardia matkapuhelin applikaatiota.



Vuonna 1998 3,6 % maailman väestöstä käytti internettiä. Nyt käyttäjiä on noin 5,35 miljardia (66,25 %).

Päivittäin maailmalla:

- Lähetetään yli 330 miljardia sähköpostiviestiä,
- Lähetetään yli 500 miljoonaa x-viestiä
- Käytetään Googlen hakukonetta 6 miljardia kertaa.

Sosiaalisen median käyttäjiä on 5,04 miljardia (62,3 %).

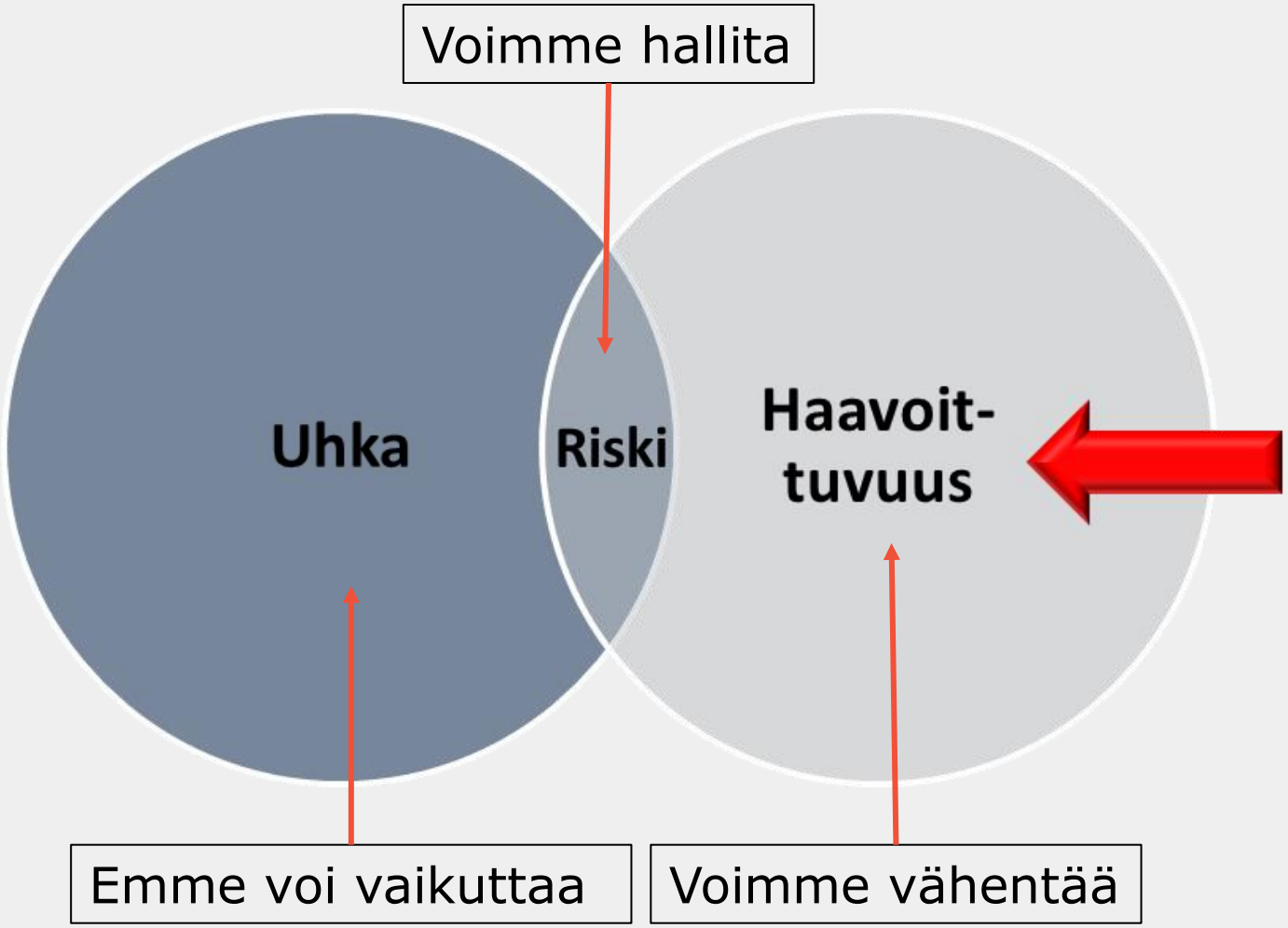
Kyber-maailma 2024

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

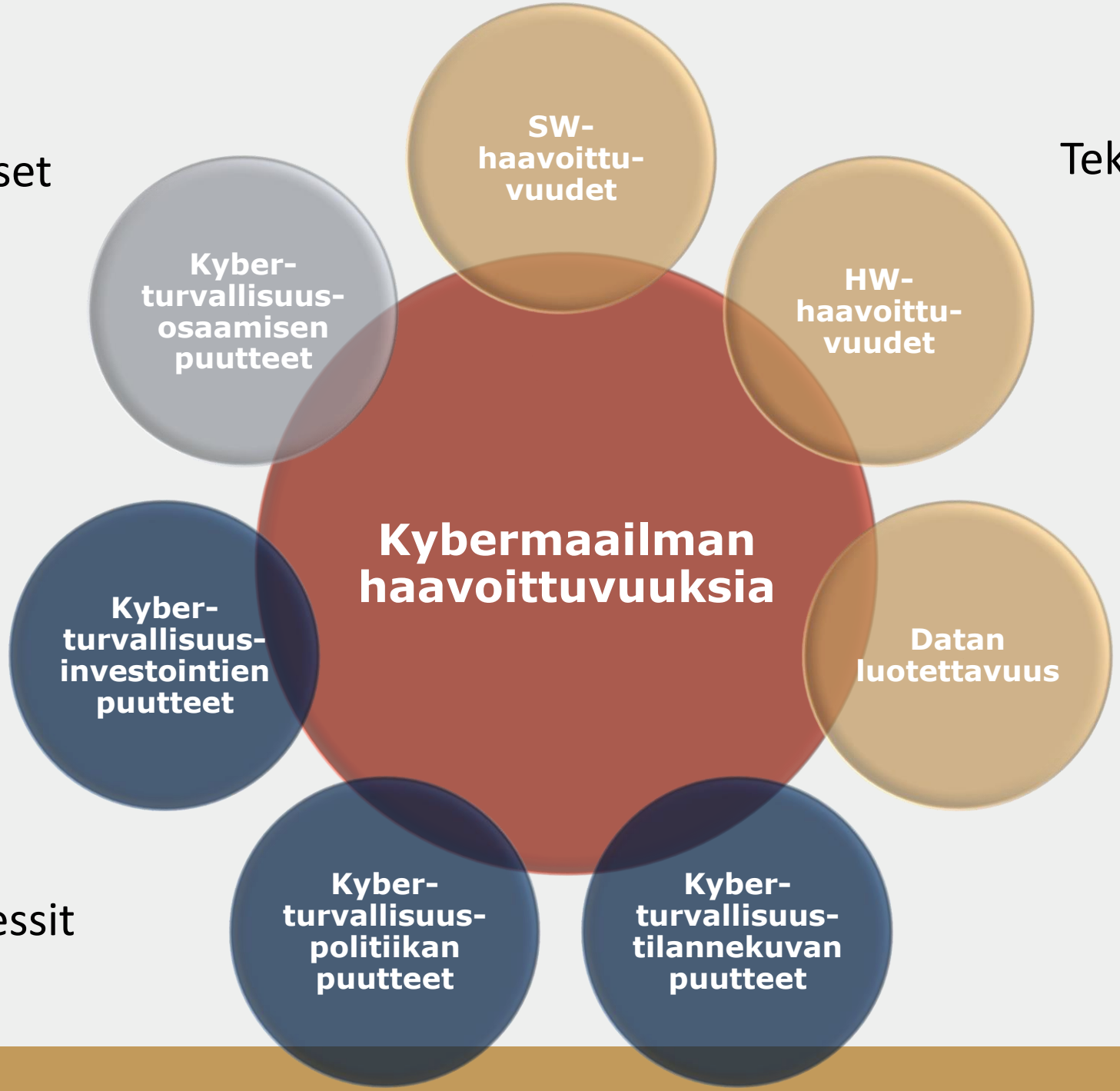
Internet | China Net | RuNet

Esityksen sisältö

Uhka + haavoittuvuus = riski

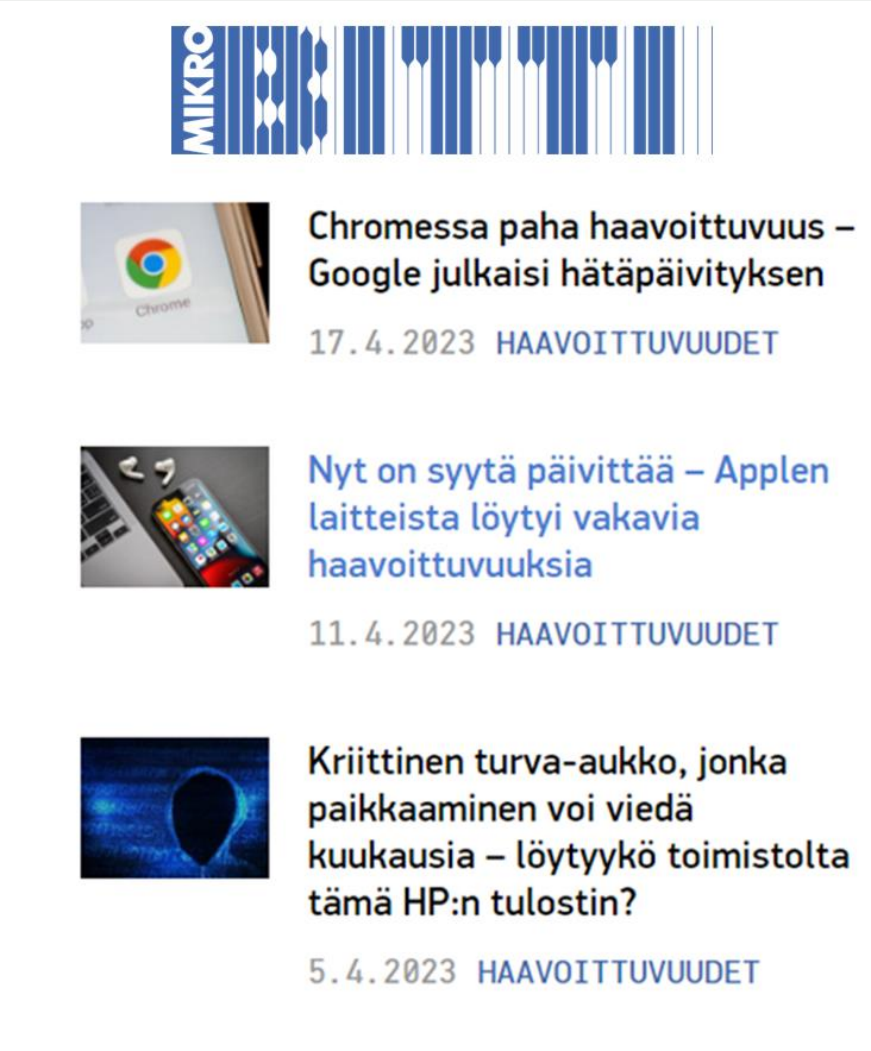


Kybermaailman haavoittuvuuksia



SW-haavoittuvuuksia

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



SW-haavoittuvuuksia

TIETOTURVA

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

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

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.

TIETOTURVA

Google Play-kaupasta löytyi vuosia piileskellyt haittaohjelma – Latasitko jonkun näistä ohjelmista?

Haitakkeen sisältämät sovellukset on sittemmin poistettu kaupasta.

Android-käyttäjiä vakoilevasta Mandrake-haittaohjelmasta on löydetty uusi versio viidestä sovelluksesta, joita on yhteensä ladattu 32 000 kertaa Google Play -sovelluskaupasta,

xz Utils - Kun koko netin turvallisuus oli uhattuna, tuuri pelasti

02.04.2024

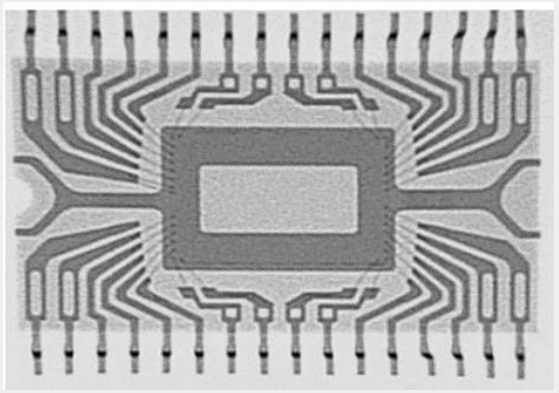
Katastrofi, jollaista ei olla voitu edes kuvitella, liittyy *Linux*-käyttöjärjestelmässä käytettyyn **xz Utils** -pakkauskirjastoon. Kyseistä kirjastoa käytetään tietoliikenteen pakkaamiseen ja se on kiinteä osa käytännössä kaikkia maailman Linux-jakeluja.

xz Utilsiin oli upotettu takaportti ja CVE-2024-3094 haavoittuvuus on luokiteltu nyt kriittisimmäksi mahdolliseksi tietoturvauhaksi mitä aukkojen asteikossa tunnetaan.

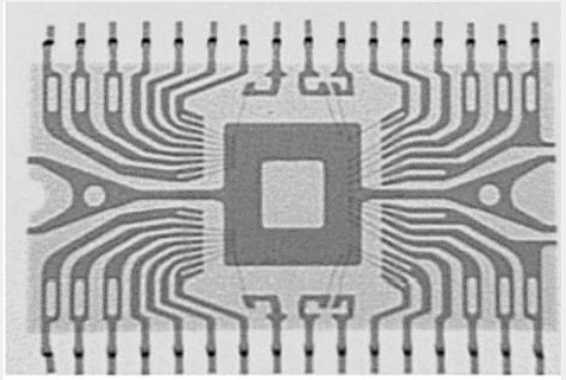
Eli takaportin avulla, tiettyjen ehtojen täyttyessä, olisi millä tahansa palvelimella voitu suorittaa mitä tahansa ohjelmakoodia, etäyhteyksien yli.

Ovatko nämä turvallisia?

HW-haavoittuvuuksia
Component corruption



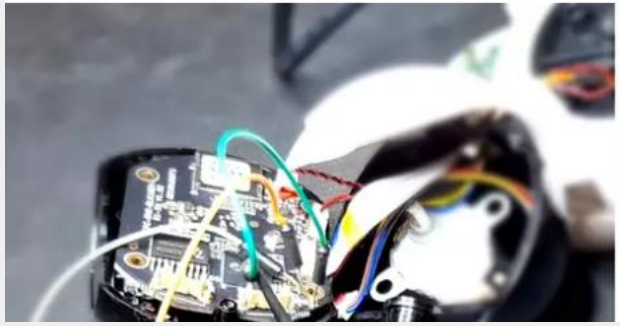
Röntgenkuvaus



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.

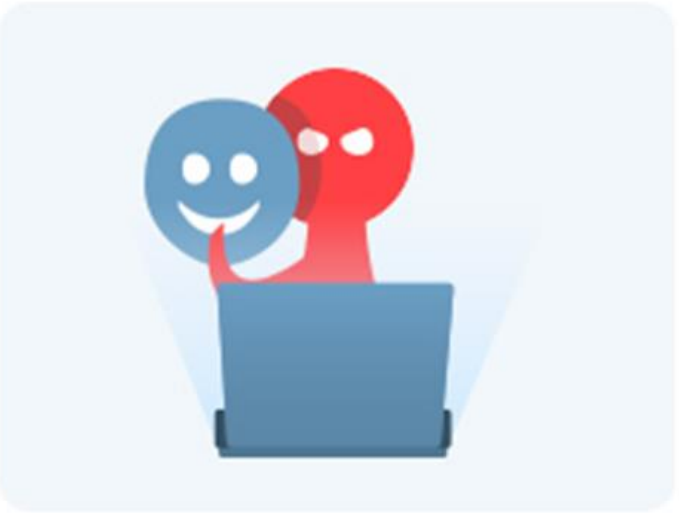
Sisäpiiriuhat

Pahantahtoinen sisäpiiriläinen

Käyttää mahdollisuutta päästä käsiksi sensitiiviseen tietoon ja tuottaa vahinkoa yritykselle.

Huolimaton sisäpiiriläinen

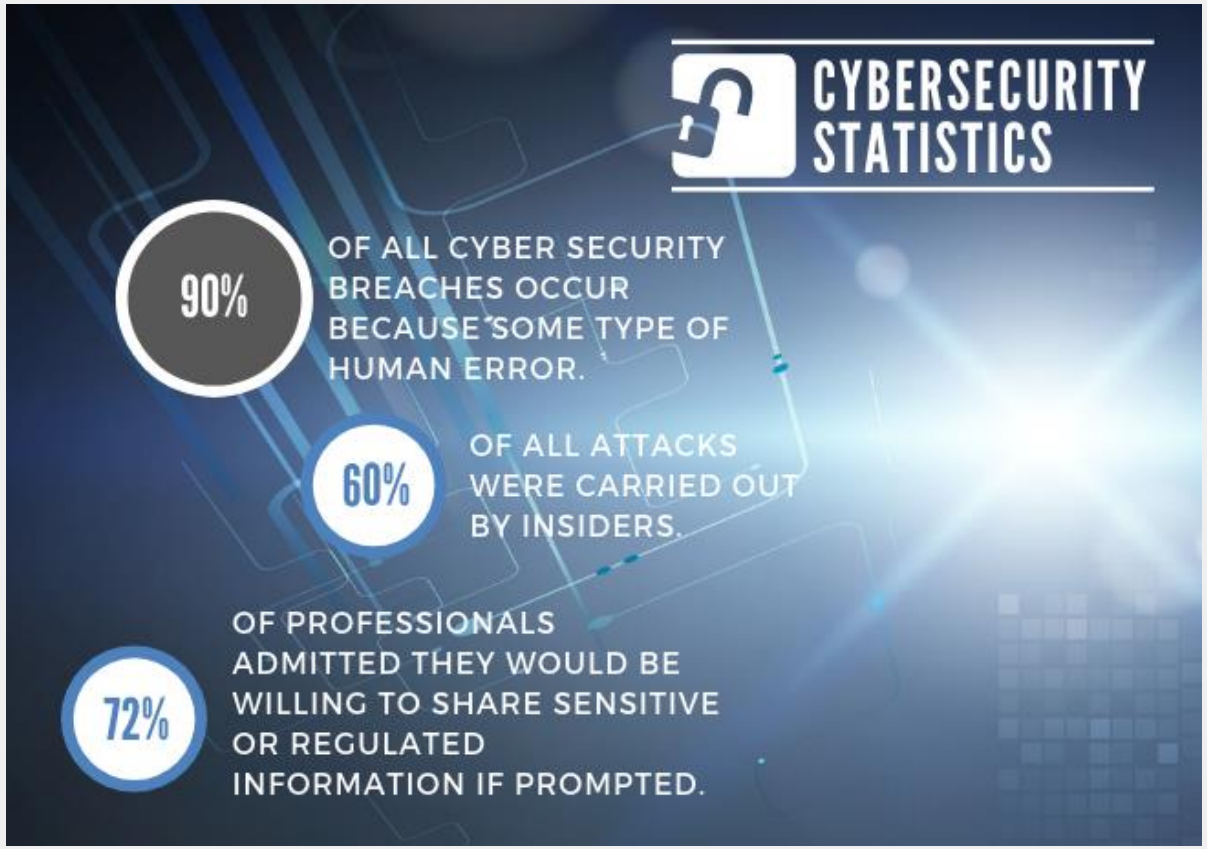
Altistaa organisaation toimimalla turvallisuusohjeiden vastaisesti



Hakkeroitu sisäpiiriläinen

Hänen käyttäjätilinsä on murrettu, vaikka hän on toiminut oikein.

Inhimilliset riskit



Lähes 90 % kyberhyökkäyksistä johtuu inhimillisestä virheestä tai toiminnasta.

Sisäpiiriläiset tekivät 60 % kaikista hyökkäyksistä.

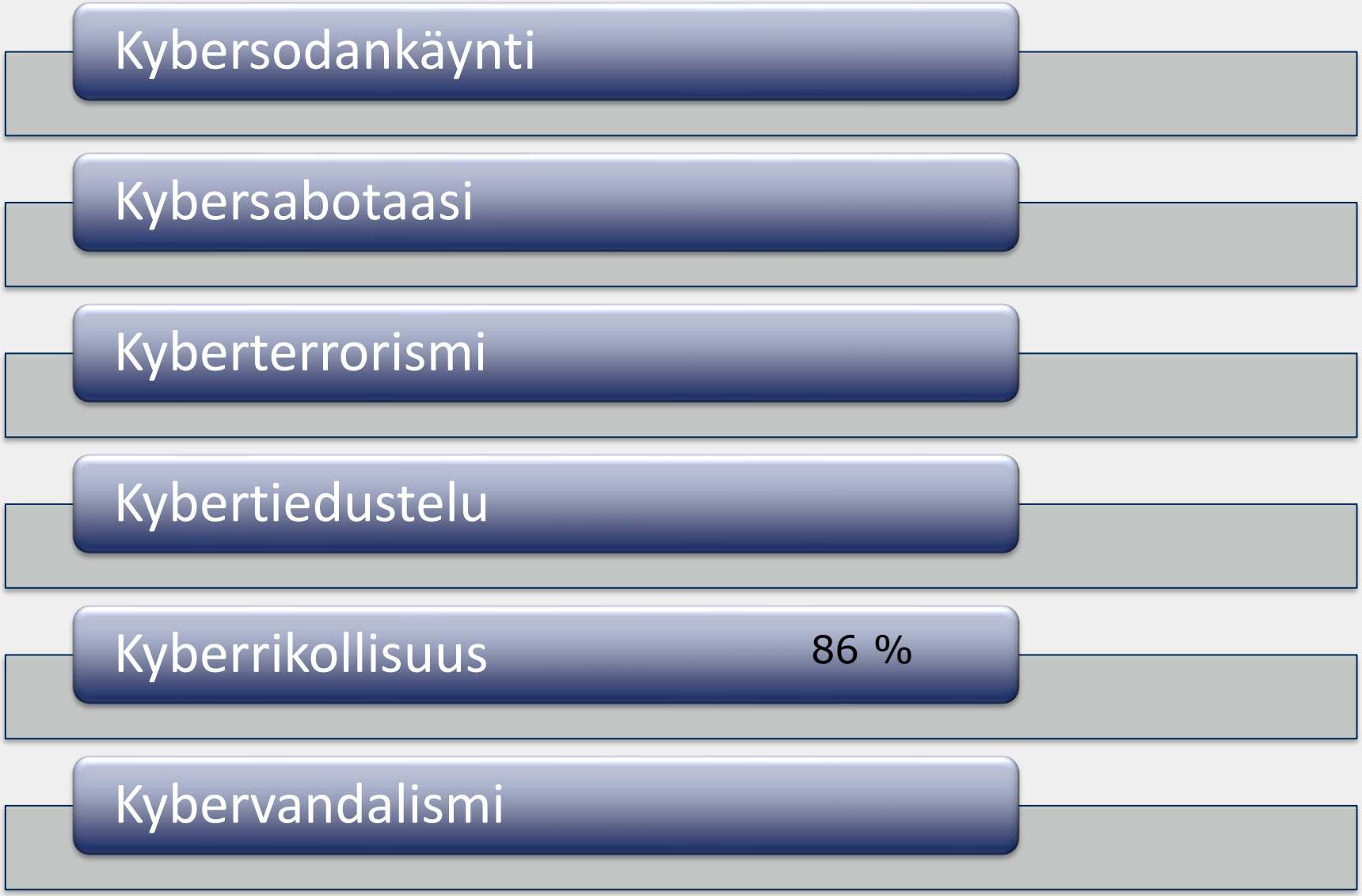
72 % myönsi, että he olisivat halukkaita jakamaan arkaluonteisia tai säänneltyjä tietoja pyydettäessä.

91 % kyberhyökkäyksistä alkaa phishing-sähköpostiviesteillä.

Source: WardSolutions: https://www.ward.ie/human-error-a-threat-in-cyber-security/

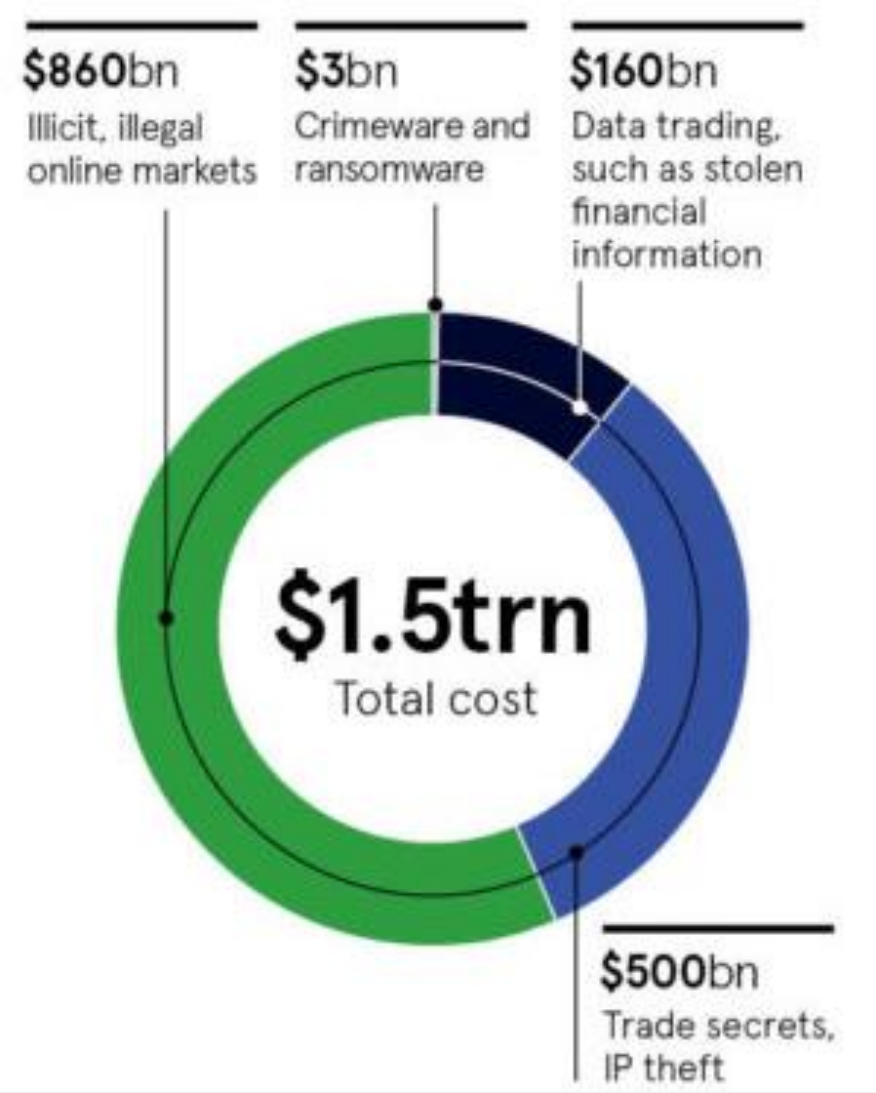
Esityksen sisältö

Kyberuhkamalli



Motivaatio ratkaisee

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

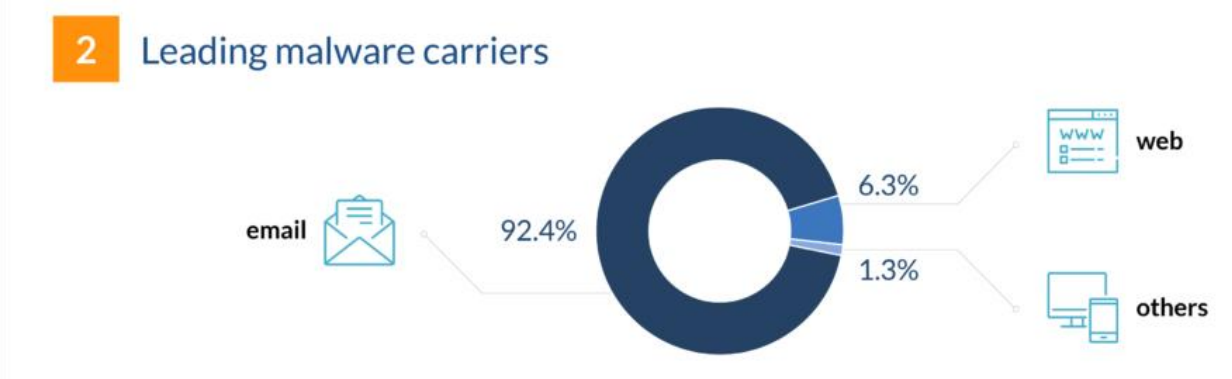
by Edvardas Mikalauskas 07 June 2021 34

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

Sähköposti on edelleen verkkorikollisten suosikkikanava

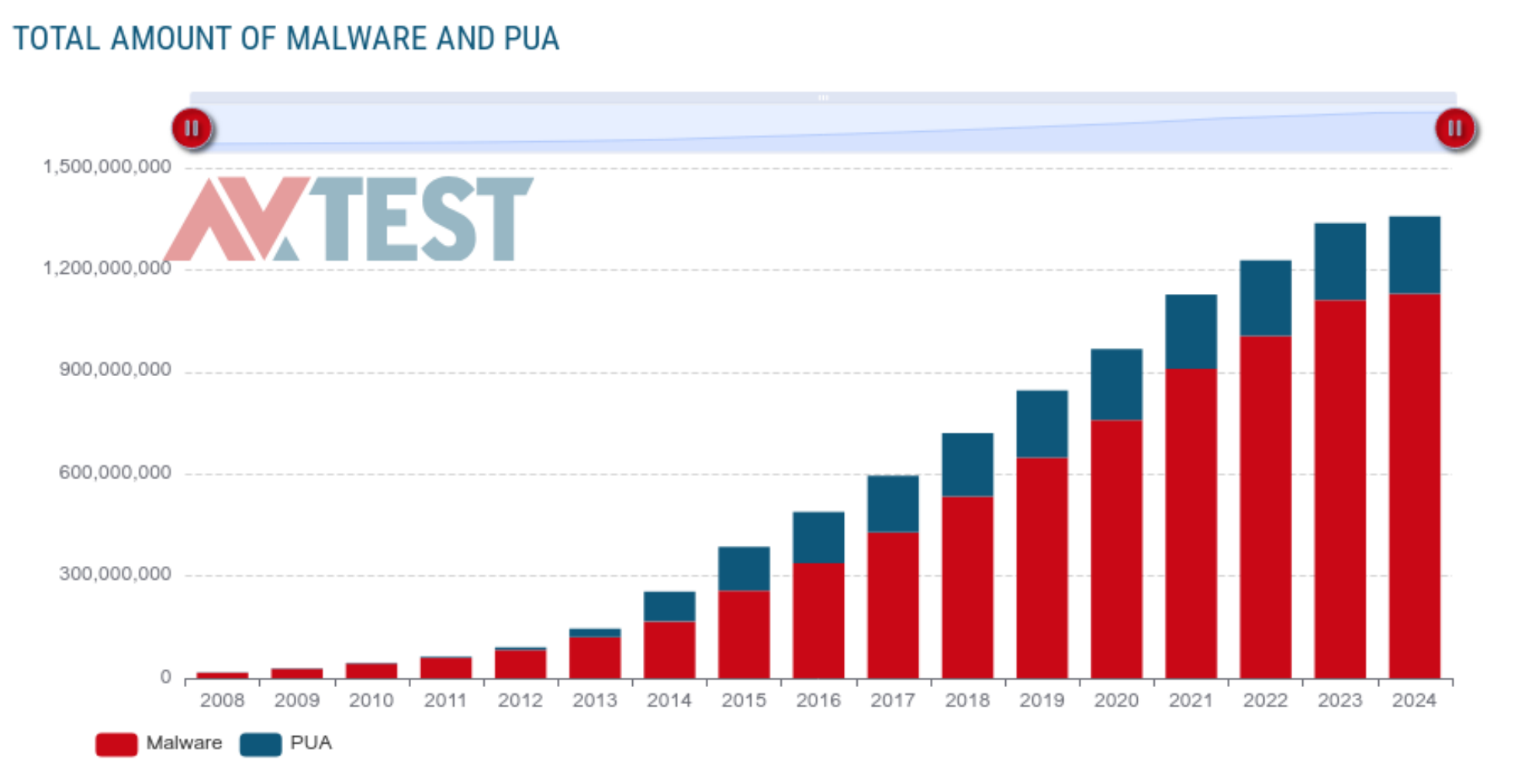
Sähköposti on eniten käytetty ja kustannustehokas sekä helppo haittaohjelmien jakelukanava.

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



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

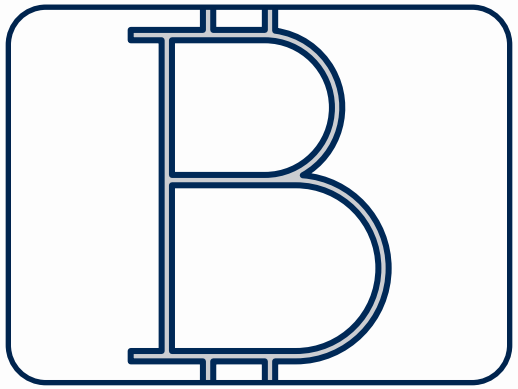
Haittaohjelmatuotanto



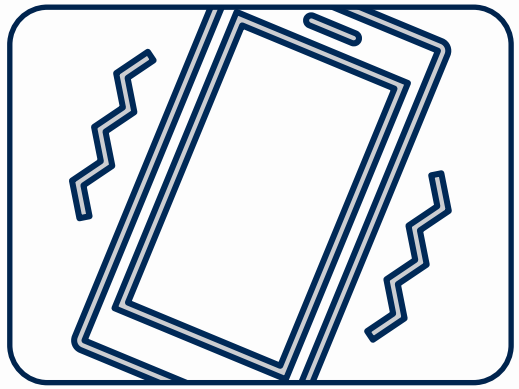
Source: AV-TEST, 20.5.2024

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

Kybertiedustelu

Julkisiin ja ei-julkisiin lähteisiin kohdistuvaa tiedonhankintaa, jonka tarkoituksena on kartoittaa ja lisätä ymmärrystä erilaisista uhista, riskeistä ja muutoksista niin maan sisällä kuin rajojen ulkopuolella.

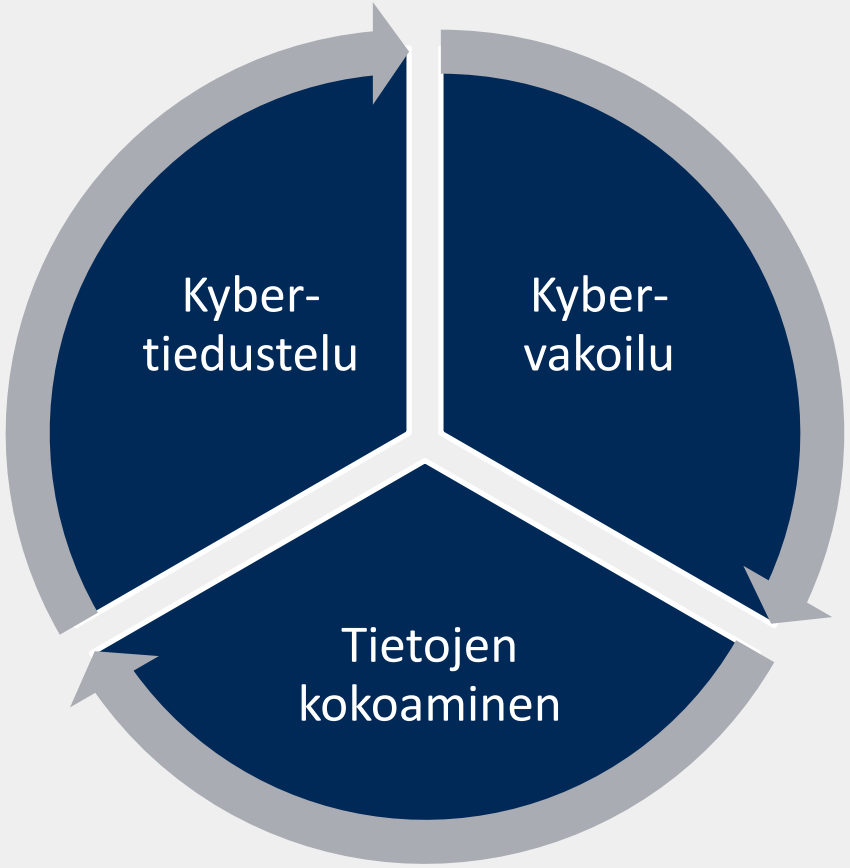
Tiedustelutoiminnan tavoitteena on tuottaa varhaisvaiheen tietoa, joka mahdollistaa uhkiin, riskeihin ja muutoksiin vaikuttamisen ja varautumisen. Tiedusteluun kuuluu tiedon analysointi, jonka avulla erilaisia turvallisuusympäristön epävarmuustekijöitä pyritään jäsentämään.

NSA US Cyber Command SRV GRU FRA SUPO

Kybertiedustelu-vakoilu-tiedon kokoaminen

Julkisiin ja ei-julkisiin lähteisiin kohdistuvaa tiedonhankintaa, jonka tarkoituksena on kartoittaa ja lisätä ymmärrystä erilaisista uhista, riskeistä ja muutoksista.

Varhaisvaroitus ja epävarmuuksien jäsentäminen.



Hankitaan salaisia tietoja yksityisiltä ihmisiltä, kilpailijoilta, ryhmiltä, hallituksilta ja vastustajilta poliittisen, sotilaallisen tai taloudellisen edun saavuttamiseksi käyttäen laittomia menetelmiä internetissä, verkoissa, ohjelmistoissa tai tietokoneissa.

Verkkokaupat, sosiaalisen median yritykset ja kehittyneet verkkopalvelut keräävät käyttäjätietoja palvelun parantamiseksi ja käyttäjän profiloimiseksi.

Avoin WLAN

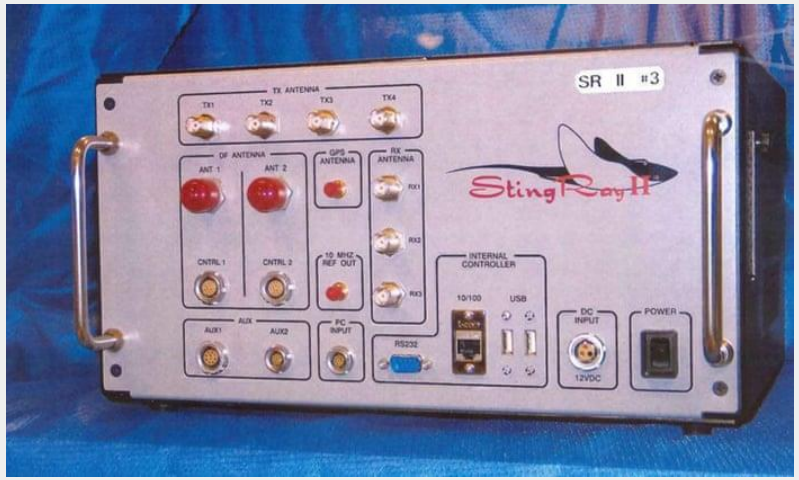
11.1.2015 Sälen

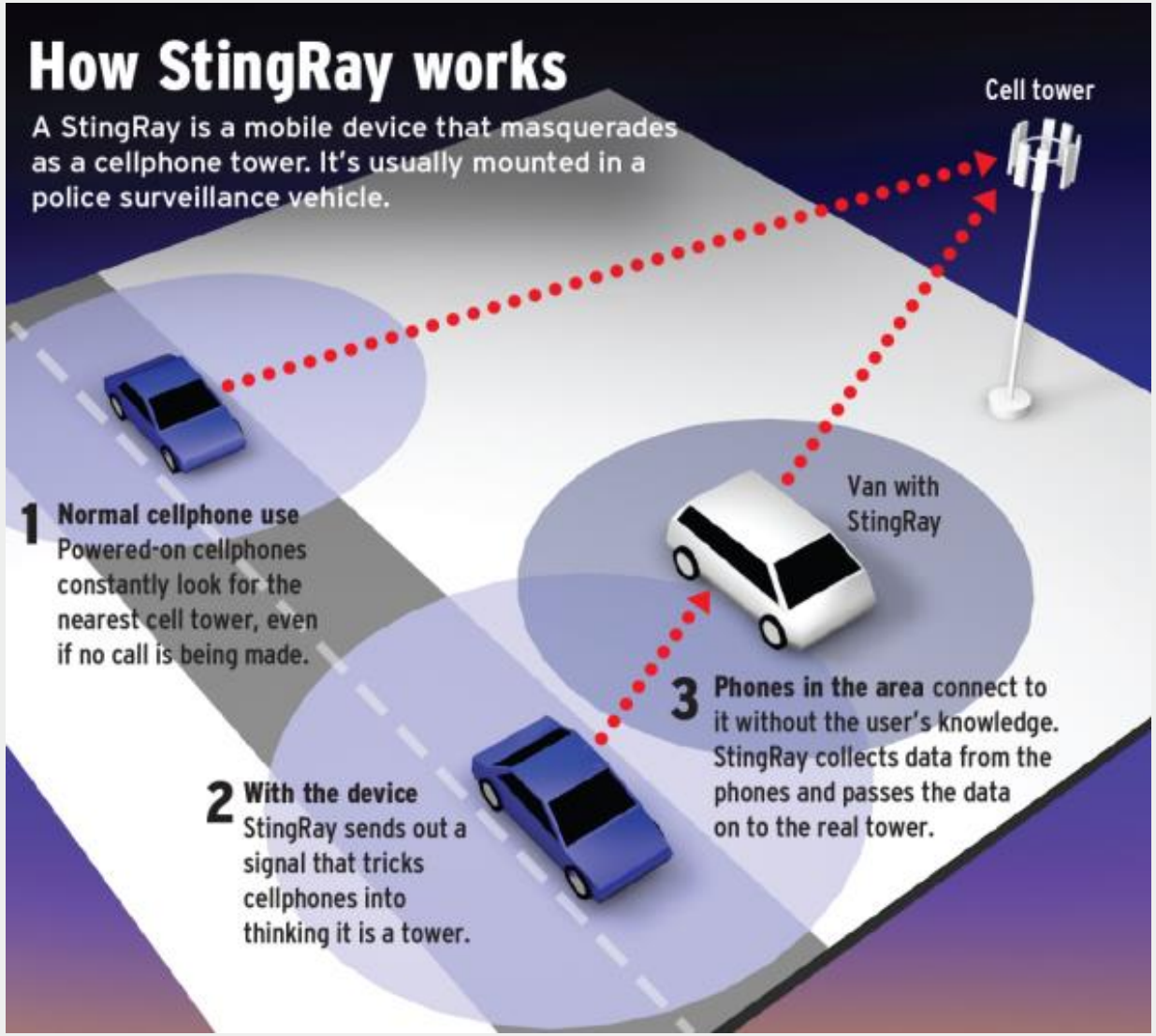
Ruotsin piraattipuolueen nuortenjärjestön puheenjohtaja **Gustav Nipe** loi puolustus- ja turvallisuuskonferenssiin wlan-verkon nimeltä Öppen Gäst.

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.

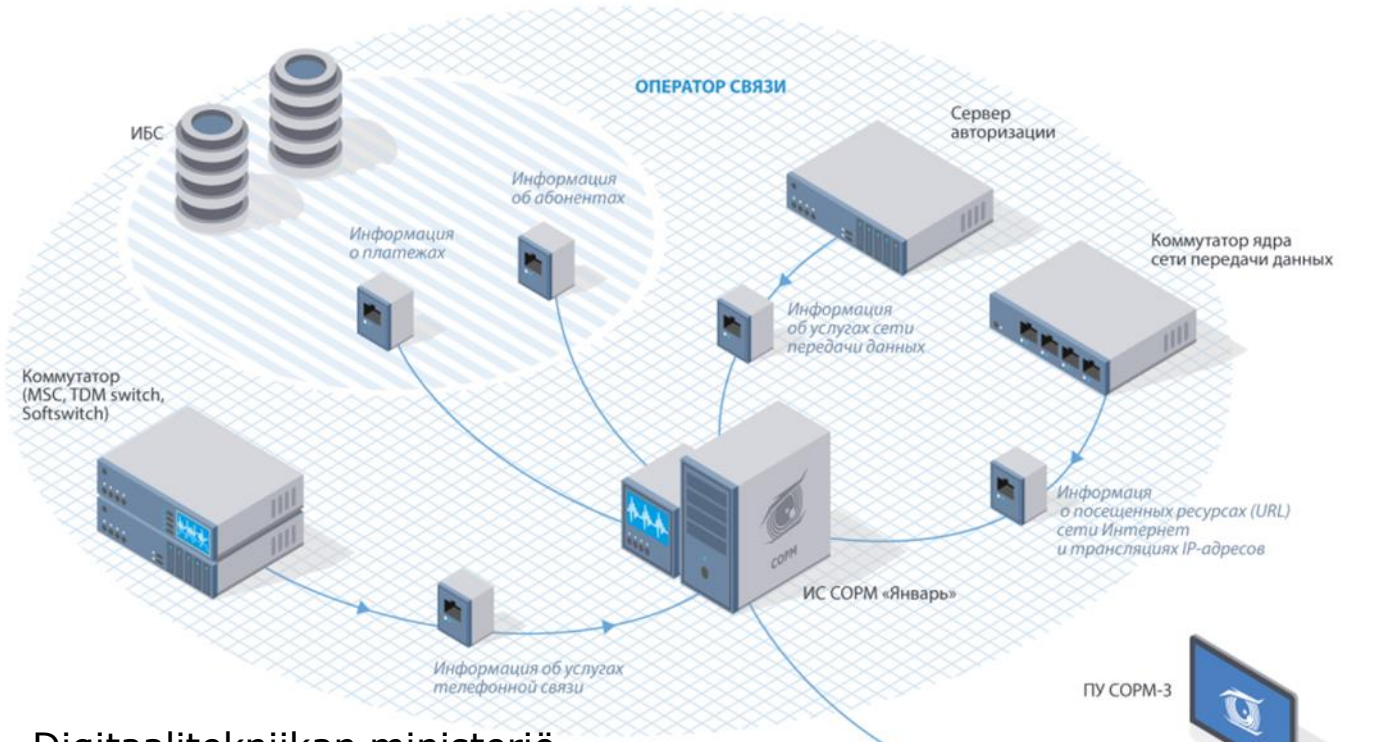
StingRay

StingRay-laite on tarkoitettu mobiilin tietoliikenteen häiritsemiseksi ja ihmisten seuraamiseksi puhelinten kautta. Laitteet teeskentelevät olevansa tukiasema ja nappaavat puhelinten tunnistekoodeja, seuraavat puhelinten sijaintia ja jopa kaappaavat puheluja ja tekstiviestejä.





SORM 3 (System of Operative Investigative Actions, COPM)



Digitaalitekniikan ministeriö, käyttöoikeus useilla ministeriöillä

SORM-3 kykenee keräämään kaiken Internetin ja mobiiliverkkojen liikenteen.

Roskomnadzor valvoo, että Internet-palveluntarjoajat asentavat FSB:n suosittelemat SORM-laitteet verkkoihinsa.

FOC 31.3.2015

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

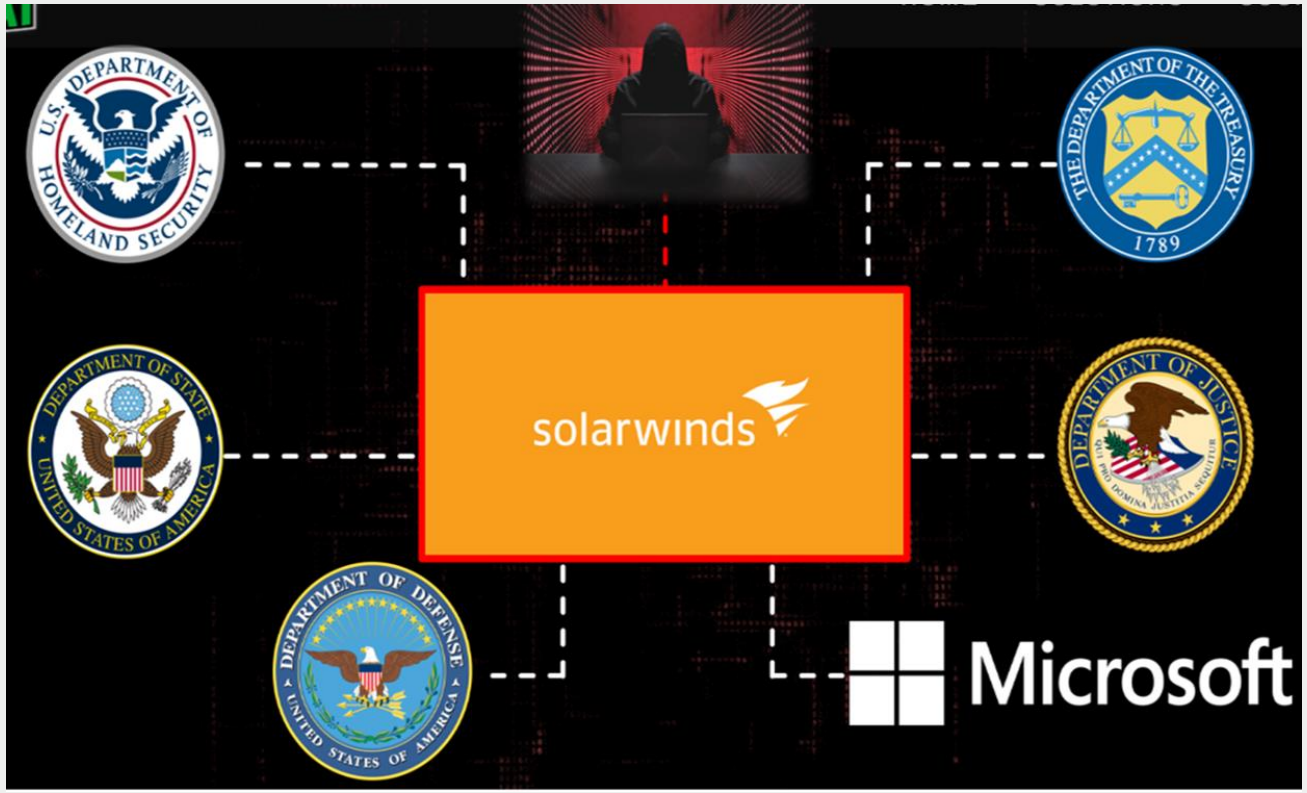
NSO Groupin Pegasus on haittaohjelma, jonka avulla voidaan mm. lukea viestejä, seurata puheluita, kerätä salasanoja, seurata sijaintia ja aktivoida mikrofoneja.

SolarWinds kybervakoiluoperaatio

SolarWinds kybervakoiluoperaatio joulukuussa 2020. Se toteutettiin toimitusketjuhyökkäyksenä, jonka kohteena olivat erityisesti yhdysvaltalaiset organisaatiot.

SolarWinds Orion on IT-infrastruktuurin hallinta- ja valvontatyökalu, joka oli vuonna 2020 käytössä noin 18 000 organisaatiossa ympäri maailmaa.

Operaation takana uskotaan olleen APT29 (Venäjän ulkomaantiedustelun (SVR) proxy).



Vihollisen järjestelmän hakkerointi

April 27, 2017, CNN

China tried to hack missile defense system

State-sponsored Chinese hackers were trying to infiltrate an organization with connections to a US-built missile system in South Korea.

The spying on the Terminal High Altitude Area Defense (THAAD) system was likely done for intelligence purposes, not to disrupt it.

Saara Aholainen HS, Hanna Freyborg HS
22.12.2022 23:53 | Päivitetty 23.12.2022 16:28

KIINALAISEN Tiktok-videosovelluksen emoyhtiö Bytedance on myöntänyt käyttäneensä Tiktokia Forbes- ja Financial Times -talouslehtien toimittajien seurantaan. Asia selvisi yhtiön sisäisessä selvityksessä.

Financial Timesin (FT) tietojen mukaan myös mediayhtiö Buzzfeedin entistä toimittajaa vakoiltiin.

Bytedancen työntekijät käyttivät Tiktokia siitä kirjoittavien toimittajien fyysisen sijainnin seuraamiseen. He pääsivät käsiksi toimittajien ip-osoitteisiin ja käyttäjädataan tarkoituksenaan selvittää, olivatko toimittajat olleet samoissa sijainneissa Bytedancen työntekijöiden kanssa.

Seurannalla Bytedance pyrki selvittämään, kuka oli vuotanut tietoja Tiktokin yhteyksistä Kiinaan.

Suosittua verkkokauppaa epäillään urkintasovellukseksi – houkuttelee asiakkaita halvoilla hinnoilla

Temusta saa tavaraa halvalla, mutta sillä voi olla omat pahantahtoiset tarkoitusperänsä.

Temun omistava *PDD Holdings* -yhtiö omistaa myös Kiinassa toimivan Pinduoduo-verkkokaupan.
Se poistettiin maaliskuussa Googlen sovelluskaupasta sen jälkeen, kun useat kyberturvallisuuden asiantuntijat, mukaan lukien suomalainen **Mikko Hyppönen**, olivat todenneet sen mahdolliseksi haittaohjelmaksi.

Turvallisuus

Viranomaiset varoittavat: Näin epädemokraattiset valtiot hyödyntävät tavallisia suomalaisia kybervakoilussa

Suojelupoliisin mukaan laittoman kybervakoilun takana ovat usein ”ei-demokraattiset valtiot”.

JESSE MÄNTYSALO

1.9. 20:15

Kuuntele juttu 4:30

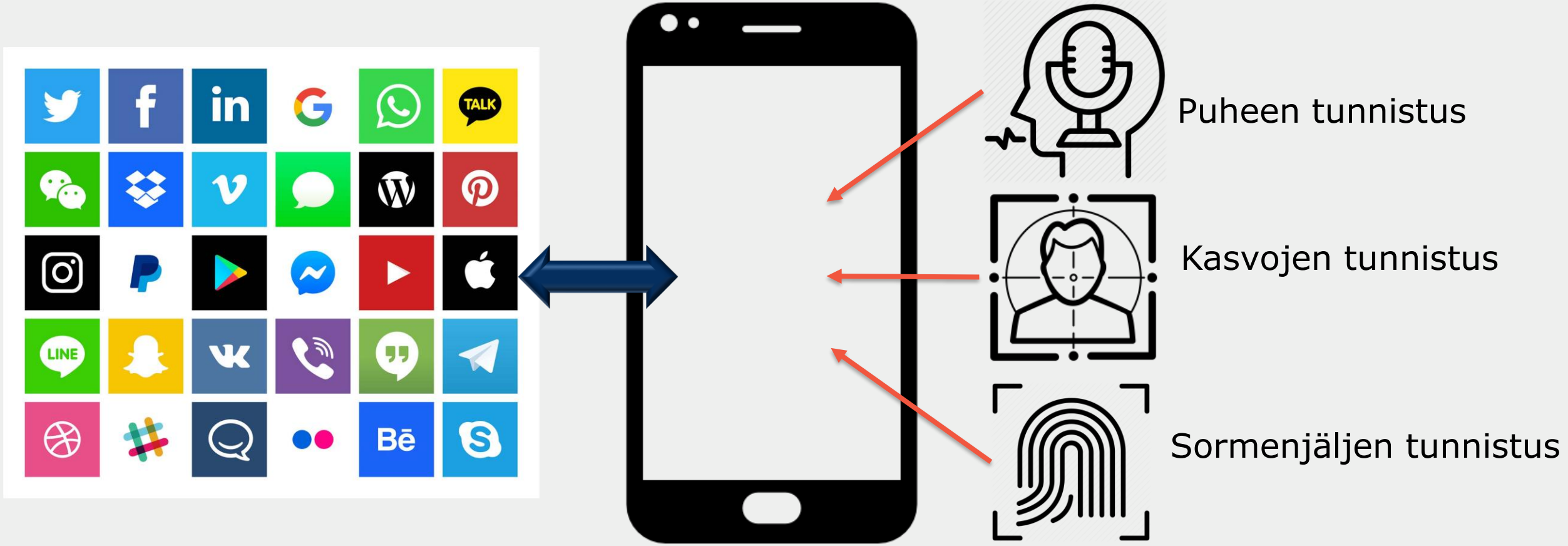
Suomalaisten kotitalouksien ja yritysten verkkolaitteisiin murtaudutaan säännöllisesti vakoilutarkoituksessa.

Suojelupoliisi (supo) varoitti viime vuonna kansallisen turvallisuuden katsauksessaan, että kuka tahansa verkkoon kiinteästi kytketyn suojaamattoman laitteen, kuten kotireitittimen, haltija voi tahtomattaan olla ulkomaisen vakoilun mahdollistaja.

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.”

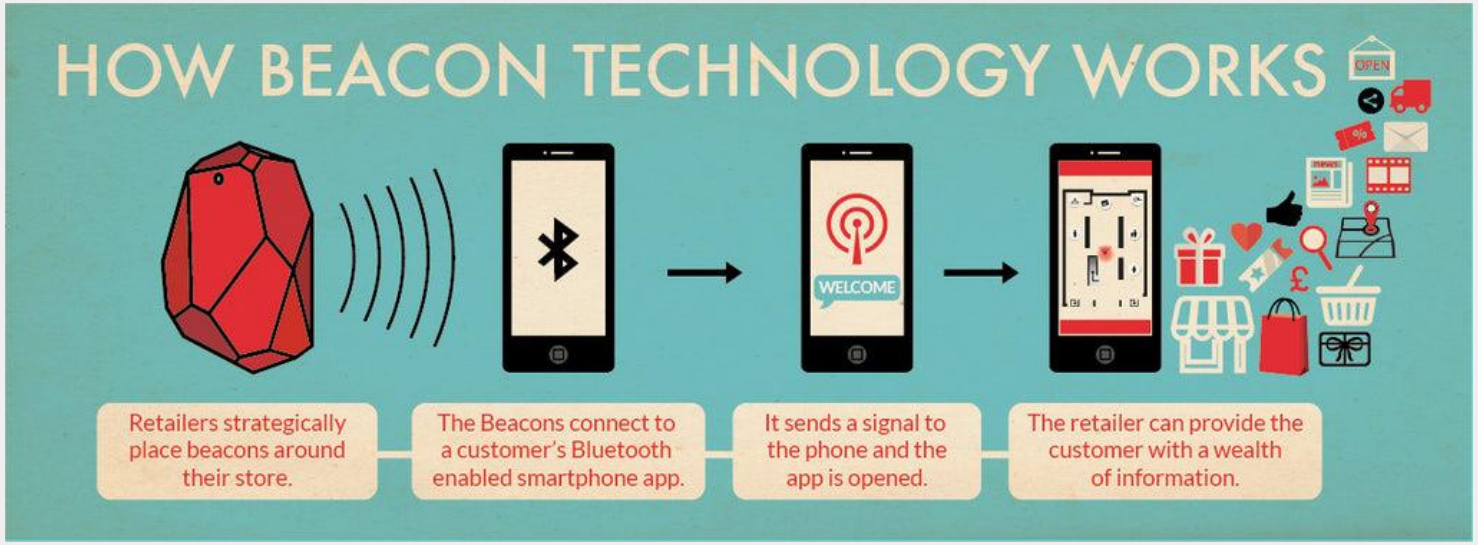
Sinun ja Googlen välinen sopimussuhde

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 kerääviä 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.”

WhatsApp käyttöehdoissa todetaan, että käyttäjä sitoutuu luovuttamaan laitteeseen tallennetut yhteystiedot palvelulle.

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

Miksi tätä tehdään?

Henkilötietojen kokoaminen - Customer Intelligence

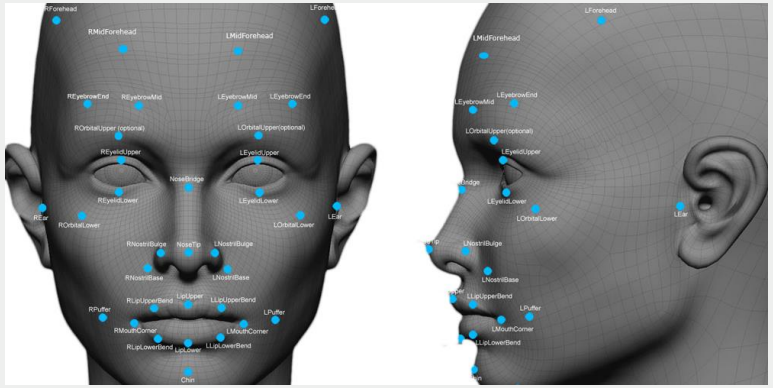
Kasvojen tunnistuksesta tunteiden tunnistukseen

Automaattinen kasvojen tunnistus ihmismassojen skannaamisen.

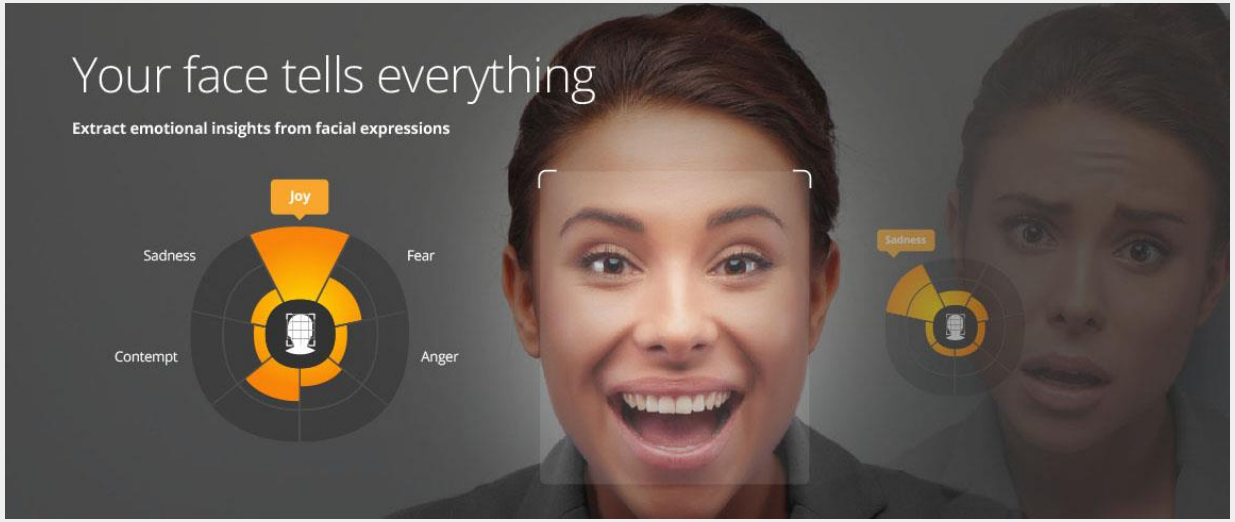
Facebook käyttää palvelussaan automaattista kasvojen tunnistusta.

Windows 10 sisältää Windows Hello –palvelun.

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



Yksilön tunnistaminen



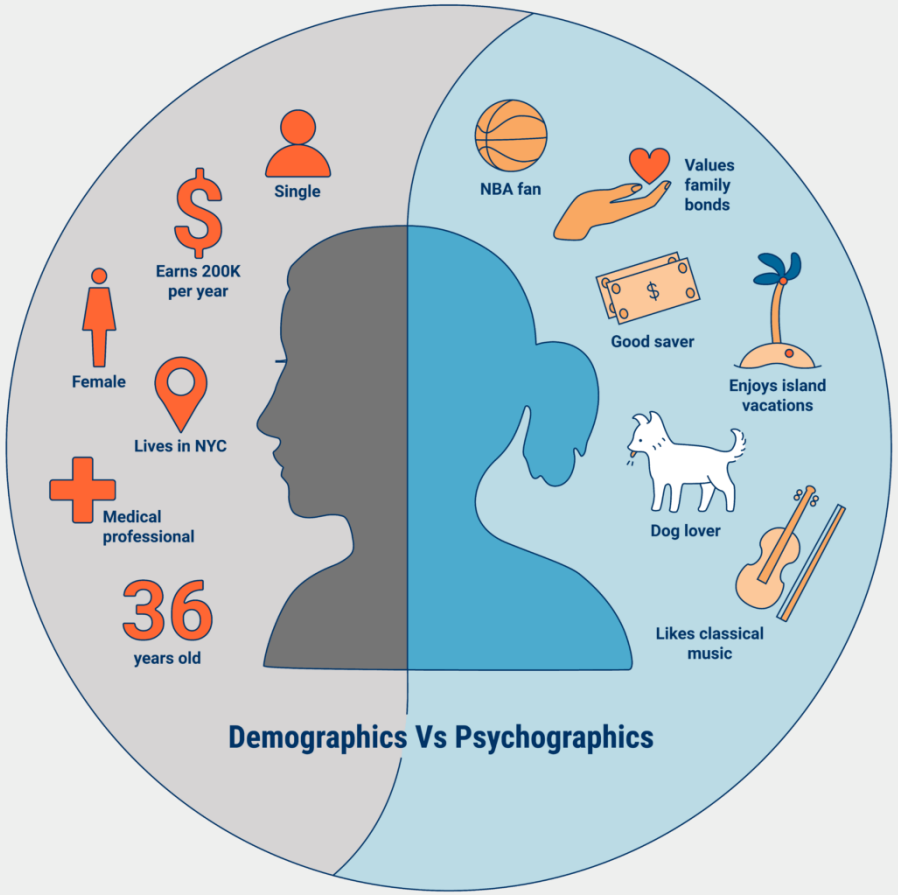
Persoonallisuuden tunnistaminen

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
- Tietomurto
- Sopimuksen vastainen käyttö

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

Twitter-vuoto pahenee: nyt 235 miljoonan käyttäjän tietoja jaetaan jo ilmaiseksi

5.1.2023 14:36

Käyttäjänimet ja sähköpostiosoitteet on kerätty todennäköisesti loppuvuodesta 2021. Joulukuussa 2022 samoja tietoja kaupiteltiin 200 000 dollarilla, mutta nyt ne ovat jaossa täysin ilmaiseksi.

Uutinen

1,38 miljoonan suomalaisen WhatsApp-käyttäjän tietoja myydään verkossa – Meta kiistää uuden tietovuodon

28.11.2022 21:06

Verkossa kaupitellaan jälleen puhelinnumeroita, mutta on hyvin mahdollista, että samat numerot ovat siellä kiertäneet jo pitkään.

Toyota mokasi taas tietoturvassa – asiakkaiden tietoja saattanut päästä vuotamaan

2.1.2023 TIETOVUODOT

Twitterissä valtavia tietovuotoja – jopa 5,4 miljoonan käyttäjän tietoja jaellaan ihan ilmaiseksi

29.11.2022 TIETOVUODOT

F-Securelta vakava varoitus: yli 200 000 suomalaisen henkilötiedot vuotaneet LinkedInistä

31.10.2022 TIETOVUODOT

DIGITODAY

Mark Zuckerberg antoi mahti-käskyn: Vakoilkaa Snapchatia, YouTubea ja Amazonia – ihmisten puhelimilla

Facebookin hanke kerätä tietoa omien palvelujensa ulkopuolella paljastui oikeudessa.

Tuomas Linnake
27.3. 13:40

METAN, eli Facebookin emoyhtiön perustaja ja toimitusjohtaja **Mark Zuckerberg** käski alaisiaan keksimään keinon vakoilla kilpailevan Snapchat-viestimen käyttäjien verkkoliikennettä sen kulkiessa Snapchat-sovelluksen ja palvelimien välillä.

Kuluttajien ja Facebookin välisessä oikeudenkäynnissä Kaliforniassa esitettiin tiistaina asiakirjoja, joiden mukaan vuonna 2016 aloitetun Ghostbusters-hankkeen tavoitteena oli selvittää käyttäjien toimintaa ja tätä kautta antaa Facebookille kilpailuetua. Myöhemmin vakoilu ulotettiin koskemaan myös Amazonia ja YouTubea.

Asiasta uutisoivat esimerkiksi TechCrunch ja Business Insider. Asiakirjojen mukaan Zuckerberg vaati selvittämään, miten Snapchatin käyttämän salauksen pystyy kiertämään todeten ”ehkä meidän pitää luoda paneeleita tai kirjoittaa omaa softaa. Teidän tulisi keksiä, miten tämä tehdään”.

Kiinan kyberturvallisuus

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

Kybermaailmassa on 0-luottamus

Luottamus ihmisiin
Autentikointi- ja auktorisointihaasteet

Component corruption
Kill Switch

Koodivirheet, bugit
Rogue applications
Back doors

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

Datamanipulaatio

Huono verkkokonfiguraatio
Verkon ”valvonta”

Esityksen sisältö

Informaatiovaikuttaminen

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

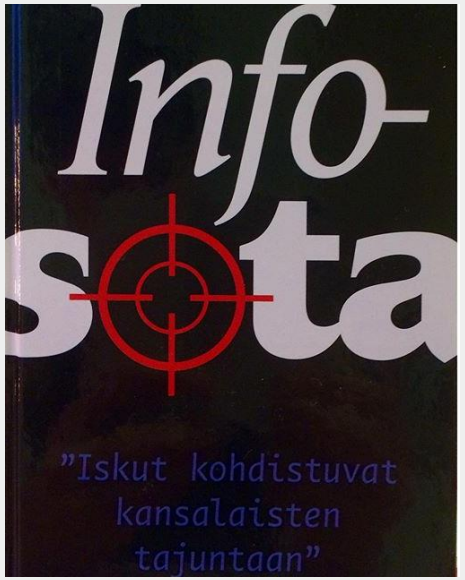
Tämä on nyt käynnissä 7/24/365

Lähde: Yleinen suomalainen ontologia 2019

Informaatiosodankäynti

Informaatiosodankäynti: vaikuttamaan informaation sisältöön ja kulkuun sekä sitä kautta eri vaiheessa olevan konfliktin tulokseen.

Käytettävät keinot voivat olla luonteeltaan strategisia, operatiivisia tai taktisia.



Informaatiosodankäynti vs. Informaatiovaikuttaminen

US Armed Forces:

"**Information Warfare** is any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions".

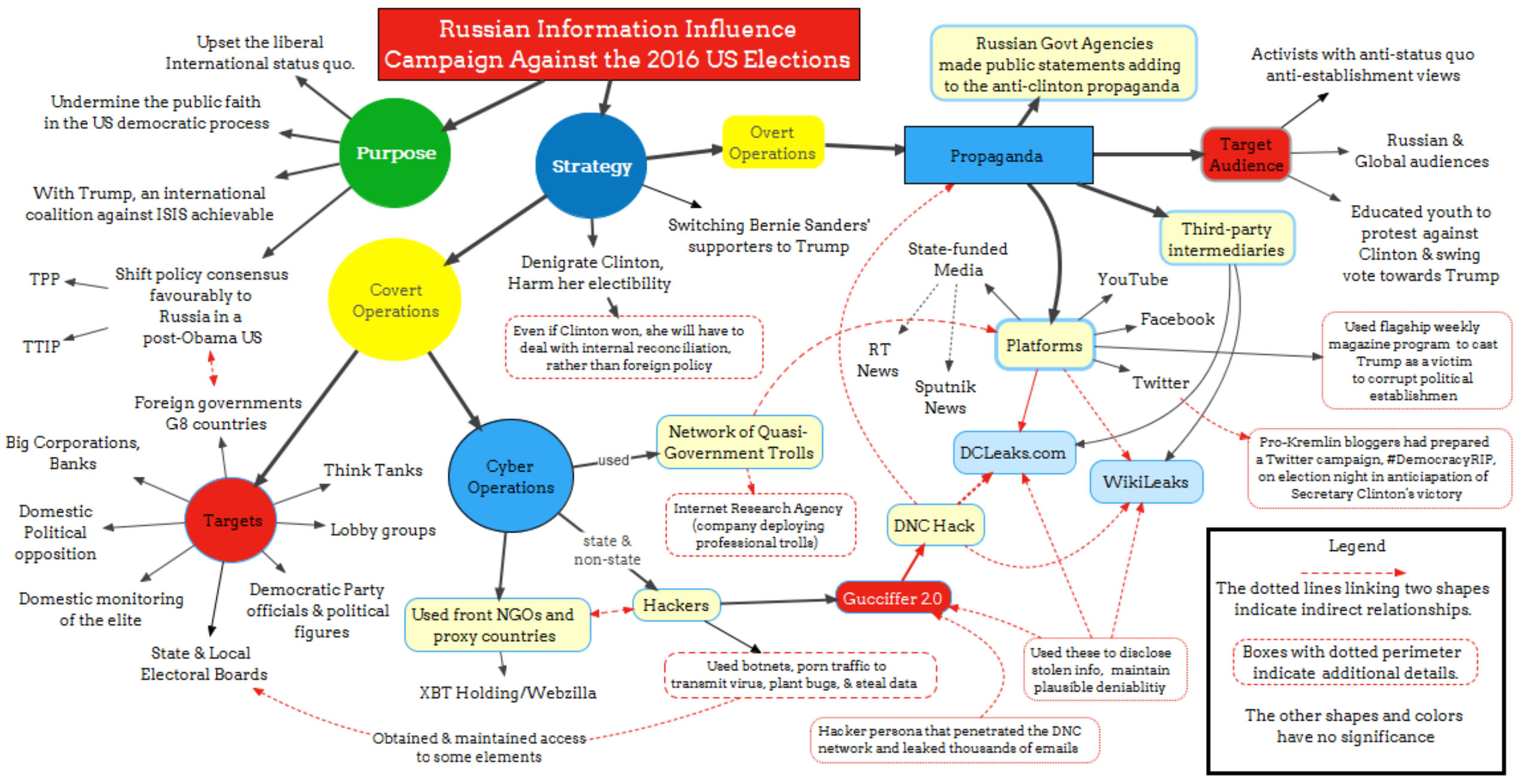
At all levels of war and at all stages of war.

Finnish Government:

"**Influencing through information** means systematic actions designed to influence public opinion, people's behavior and decision-makers and, through that, the functions of society."

The methods include fake news, disinformation, trolling, or manipulative use of information.

AT WAR INTERNET OCCURS 24/7

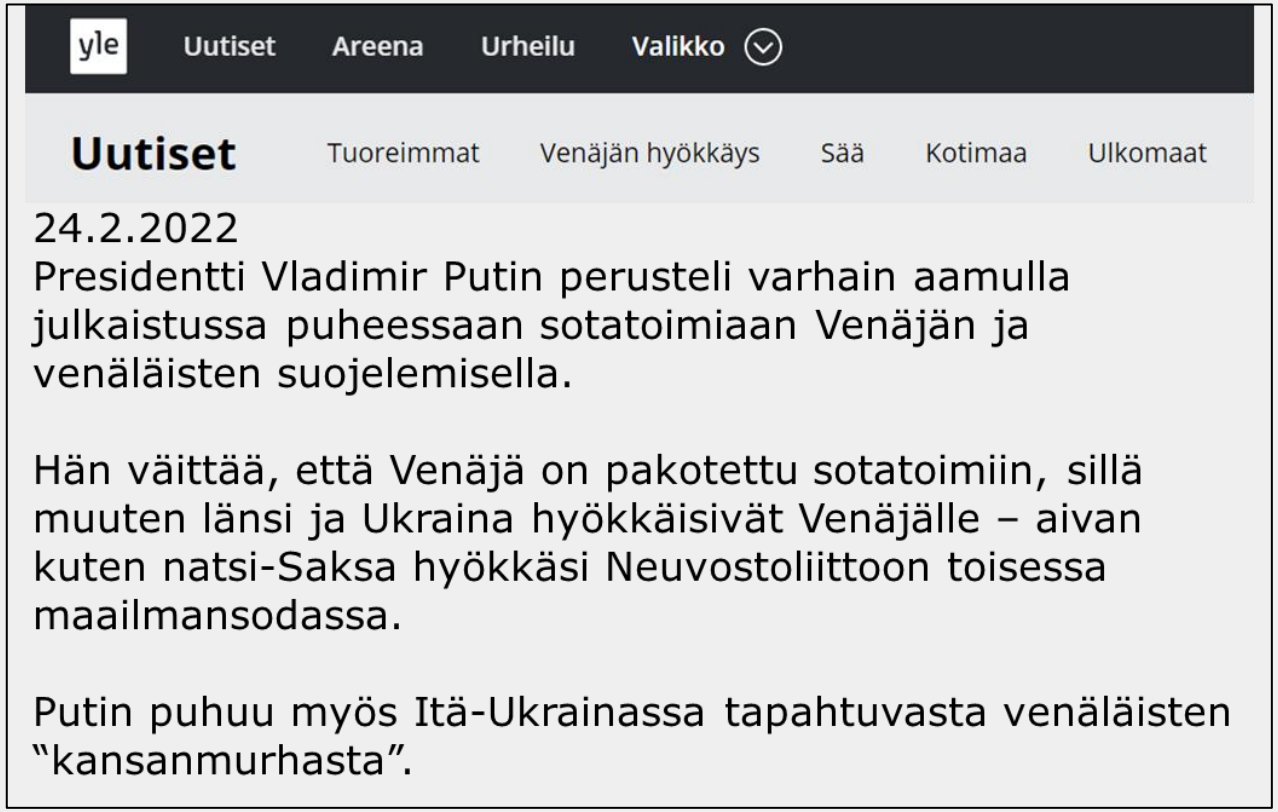


Mind map of the Russian Influence Campaign on the US 2016 Presidential Elections

by Puru Naidu on January 17, 2017, in BLOG

Strateginen kommunikaatio

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


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".

Informaatio-operaatiot

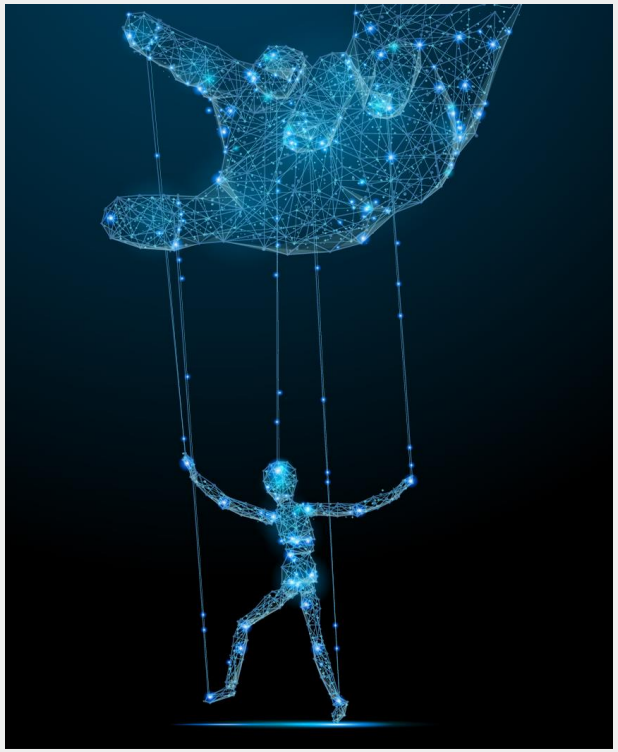
Tavoitteena on vaikuttaa sodan lopputulokseen.

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*

Laaja keinovalikoima mediassa ja somessa.

Kaikilla sodankäynnin tasoilla ja kaikissa sodan vaiheissa.



Informaatio-operaatiot

1. Harhauta ja petä kohdehenkilöä/ -yhteisöä

- Käyttäydy kuin oikea media/näytä oikealta medialta

2. **Hyödynnä järjestelmän haavoittuvuuksia**

- Mielipiteen ilmaisunvapaus
- Avoin sosiaalinen media
- ”usko tiedotusvälineisiin”

3. **Riko sääntöjä**

- Valehtele
- Trollaa

Sergei Lavrov syyttää Ukrainaa ja länttä Butšan raakuuksista: ”Valehyökkäys”

4.4.2022 17:15 | päivitetty 4.4.2022 17:15

UKRAINAN KRIISI TURVALLISUUSPOLITIIKKA TURVALLISUUS MAANPUOLUSTUS ULKOPOLITIIKKA

Ukrainan Butšassa paljastui silmittömiä raakuuksia, jotka on tuomittu laajalti. Venäjän ulkoministerillä on oma versionsa tapahtumista.

Informaatiopuolustuksen torjunnan kehittäminen

Puolustusselonteko:
”Informaatiopuolustuksen päämäärä on suojata maanpuolustuksen toimintoja.”

Sisäisen turvallisuuden selonteko näkee informaatiovaikuttamisen yhteiskunnan yleisen järjestyksen ja turvallisuuden näkökulmasta.

Kenen vastuulla on koko yhteiskuntaan kohdistuvan informaatiovaikuttamisen torjunnan toteuttaminen?

Esityksen sisältö

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

Kyberoperaatioita Ukrainassa

2022: Yhteensä 254 2023: Yhteensä 412

Tuhoavat hyökkäykset: tarkoituksena on tietojen pysyvä poistaminen tai järjestelmien vahingoittaminen pysyvästi.

Häiritsevät hyökkäykset, joiden tarkoituksena on häiritä palveluita ja toimintaa. Hajautetut palvelunestohyökkäykset (DDoS) ovat olleet yleisimpiä. Ne muodostivat 87,5 % kaikista tammi-maaliskuussa 2023 analysoiduista kyberhyökkäyksistä.

Tiedusteluhyökkäykset, joissa varastetaan tietoja eri tarkoituksiin, kuten hyökkäysten kohdistamiseen, vaikutusten analysointiin ja vakoilutarkoituksiin. Kohdistettu myös muihin länsimaihin.

Disinformaatio-operaatiot jotka keskittyvät väärän tiedon levittämiseen ja propagandaan. Uhkatoimijat pyrkivät vaikuttamaan informaatioympäristöön ja rajoittamaan väestön oikea-aikaisen, luotettavan ja virallisen tiedon saatavuutta tai tarkoituksellisesti hämärtävät ja heikentävät tiedon saatavuutta.

Ukrainassa:
- 166 miljoonaa disinformaatio-viestiä viikossa.
- 50 000 somen fake-profiilia Ukrainaa vastaan.

Näkemys tilanteesta

”Suurin osa Venäjän kyberhyökkäyksistä näyttää olevan nimenomaan tarkoitettu häiritsemään arjen rutiineja esimerkiksi katkaisemalla sähköt tai tekemällä Internet-yhteydet epävakaiksi. Hakkerien tavoitteena on tehdä elämästä niin epämukavaa, että ukrainalaiset menettävät toivonsa itseensä, menettävät uskonsa johtajiinsa ja lopulta luopuvat taistelusta itsenäisyydestään ja alueestaan.

Niin oudolta kuin se saattaakin tuntua, Moskova on tehnyt siviilien demoralisoimisesta kyberavaruudessa keskeisen pilarin sille, miten se ajattelee sotien voittamisesta.”

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

Source: Gavin Wilde, Why Cyber Attacks on Ukrainians Aren’t Working the Way Russia Expected, Blog, Carnegie Endowment for International Peace, March 11. 2024.

Supon päälliköltä vakava varoitus Suomelle: ”Nyt kaikkien on todellakin oltava hereillä”

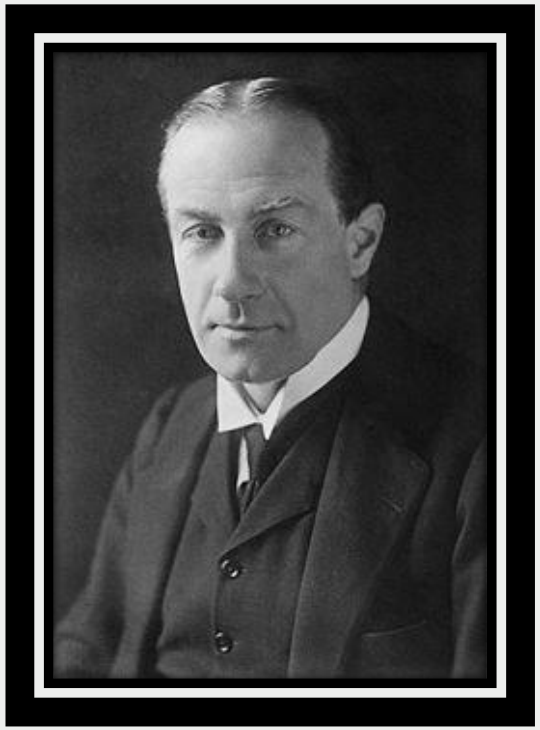
Suojelupoliisiin päällikkö Antti Pelttari varoitti jo vuosi sitten, että Venäjä ja Kiina yrittävät päästä kiinni Suomen kriittiseen infrastruktuuriin.

IL Keskiviikko 23.3.2022 klo 11:45 (muokattu 26.3.2022 klo 11:15)

Entä millaisia uhkia on nyt, kun Venäjän hyökkäyssota on jatkunut Ukrainassa jo kuukauden?

Mihin kaikkeen Suomessa pitää varautua nyt ja tulevaisuudessa? Suojelupoliisiin päällikkö **Antti Pelttari** vastasi kysymyksiin suorassa Sensuroimaton Päivärinta -lähetyksessä.

”Pommittaja pääsee aina läpi”

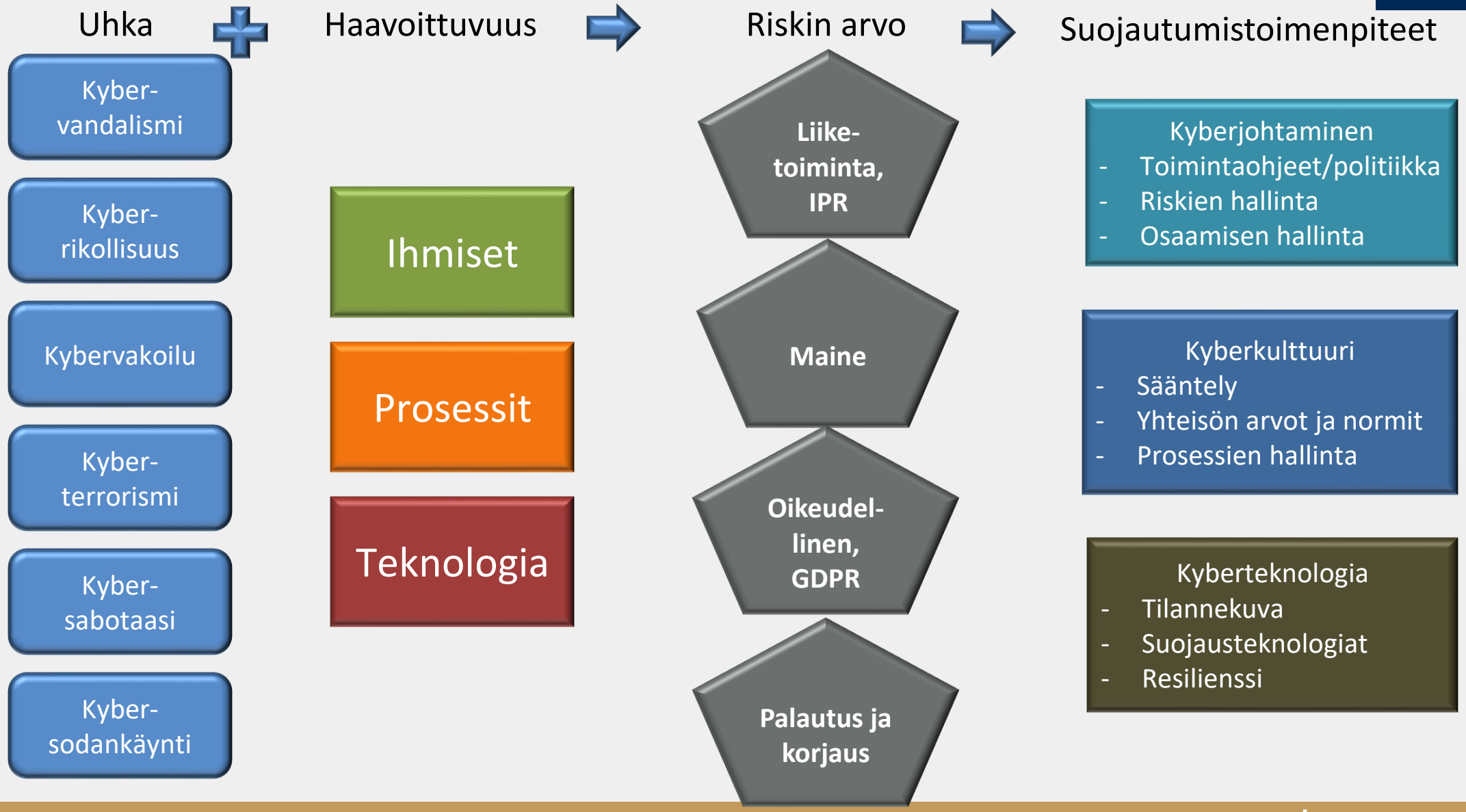


Prime minister **Stanley Baldwin**: "*It is well for the man in the street to realise that there is no power on earth that can protect him from being bombed... **the bomber will always get through***."

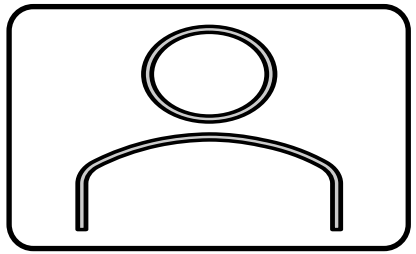
Speech in House of Commons of the Parliament of Great Britain in November 1932.

→ ”Kyberhyökkäys pääsee aina läpi”

Kyberturvallisuuden rakentaminen

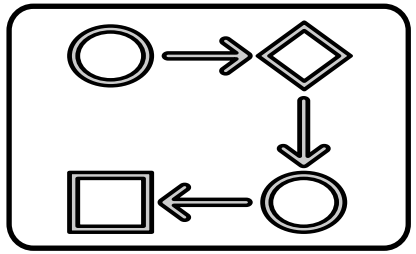


PPT-vahvistaminen



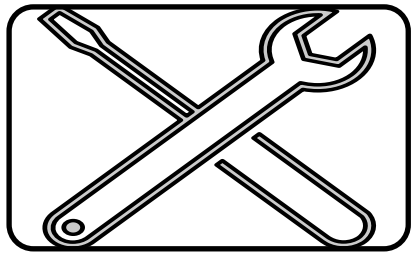
Ihmiset

- Työntekijöiden osaamisen kehittäminen
- Kyberammattilaisten käyttö ja resurssointi
- Sertifikaatit



Prosessit

- Selkeä kyberturvallisuuden johtamisprosessi
- Organisaation kaikkien prosessien hallinta (normaali – epänormaali)
- Riskien hallinta - häiriötilanteiden hallinta – jatkuvuuden hallinta



Teknologia

- Kyberturvallisuusarkkitehtuuri
- Tietojärjestelmäympäristön tilannetietoisuus
- Sertifioidut kyberturvallisuuden laitteet ja ratkaisut

Kiitos

www.jyu.fi/it