JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Mitä jokaisen opetusalan ammattilaisen pitää tietää kyberturvallisuudesta?

Professor of Practice, ST, ev evp. Martti Lehto

26.9.2019

Kyberosaaminen

Varhais-kasvatus

Yleis-sivistävä perusopetus

Lukio-koulutus

Ammatilli-nen koulutus

Korkea-koulutus

Aikuis-koulutus

Mitä jokaisen tulisi tietää kyberturvallisuudesta?

Kyberturvallisuuden opetus

Kyberturvallisuuden maisteriohjelmassa korostuvat kyberturvallisuuden suunnittelu, johtaminen ja kyberturvallisuusriskien hallinta niin johtamisen kuin teknologiankin näkökulmasta.

1. Kyberkonfliktien hallinta
2. Kyberturvallisuus yhteiskunnassa
3. Informaatiovaikuttaminen
4. Anomaliat ja niiden havaitseminen
5. Kyberfyysisten järjestelmien resilienssi
6. Julkisen hallinnon kyberturvallisuus

Esityksen sisältö

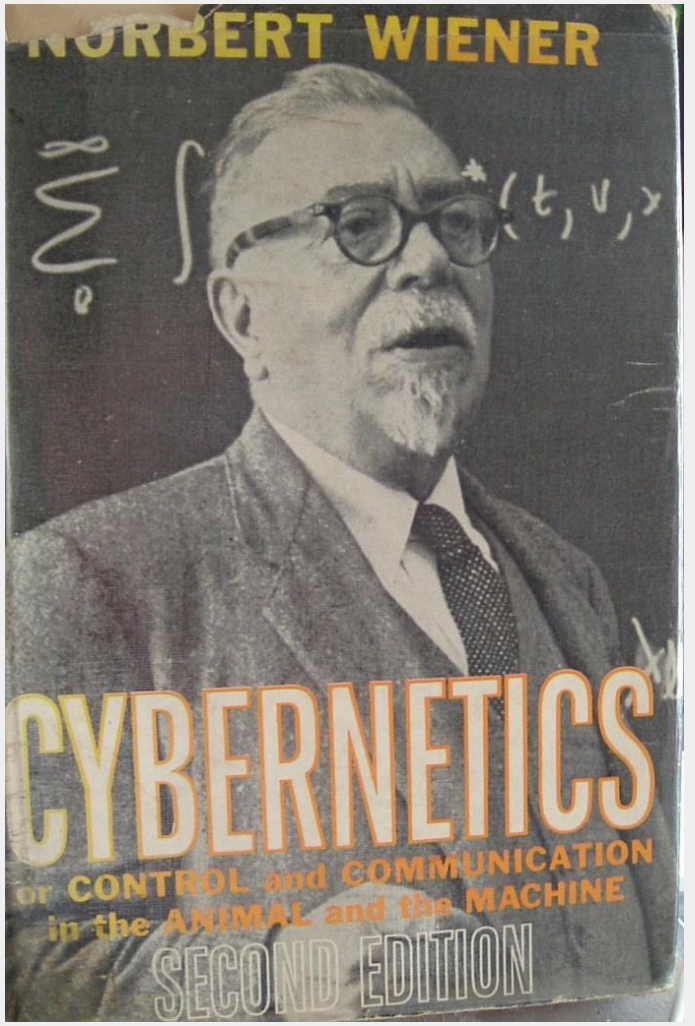
1. Digitaalisen maailman muutos
2. Kybermaailman uhkia
3. Kybermaailman haavoittuvuuksia
4. Kybermaailma ja ihminen
5. Turvallisuuden rakentaminen

Kybermaailman määrittelyä

Sana kyber tulee kreikan sanasta "kybereo" - ohjata, opastaa, hallita.

Amerikkalainen matemaatikko **Norbert Wiener** (1894–1964) otti käyttöön sanan kybernetiikka 1940-luvun lopulla kuvaamaan tietokoneita käyttäviä ohjausjärjestelmiä.

Hänen mukaansa kybernetiikka kuvasi tieteitä, jotka käsittelevät koneiden ja organismien kontrollointia kommunikaation ja palautteen avulla.

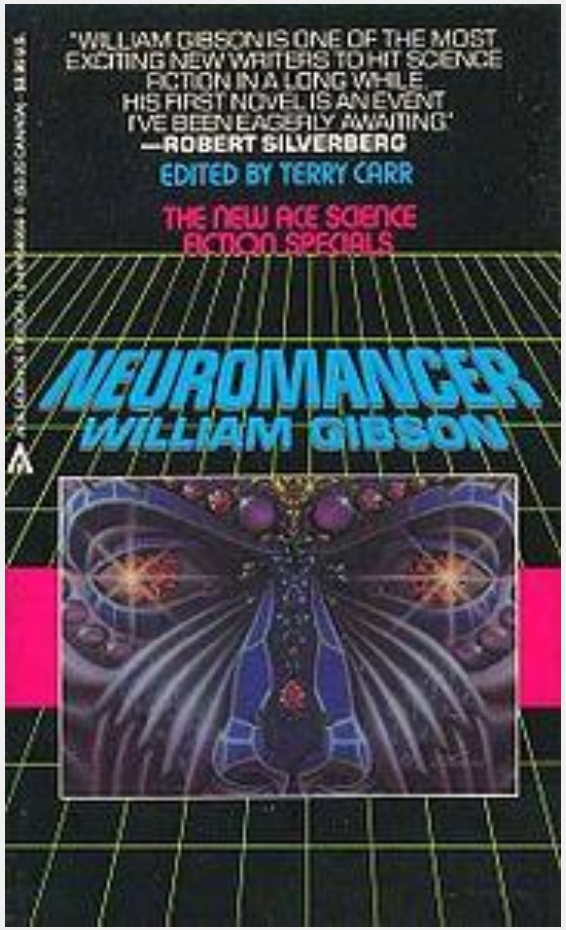


Kybermaailman määrittelyä

Sanan kyberavaruus keksi tieteiskirjailija **William Gibson** (7.3.1948-) 1984 kirjassaan Neuromancer.

Gibsonilainen kyberavaruus esitetään globaalina informaation tietokoneverkkona, jossa käyttäjä voi liikkua virtuaalihahmossa.

Matrix-elokuva: 1999



Mikä on muuttunut?

Aika

Data

Verkko

Älykkyys

Robotiikka

Pörssimanipulaatio

Huhtikuussa 2013 syyrialaiset hakkerit kaappasivat uutistoimisto AP:n Twitter-tilin ja twiittasivat presidentti Barack Obaman haavoittuneen räjähdyksessä Valkoisessa talossa.

New Yorkin pörssin Dow Jones Industrial Average -indeksi romahti hetkessä 130 pistettä.

Pörssirobotit myivät valtavat määrät osakkeita ennen kuin yksikään ihminen ehti reagoida tekaistuun uutiseen.

Datan luonti

Olemme luoneet dataa ihmiskuntana vuoteen 2003 mennessä noin 5 eksatavua.

Nyt luomme noin 10 eksatavua joka päivä.

- NY Stock Exchange: 1TB/päivässä
- The Large Hadron Collider (CERN), 150 milj. Sensoria: 22 PB vuodessa (2012)
- Facebook: 40 miljardia kuvaa, 4PB

1 EB = 10^{18} bytes = 1000000000000000000

Kriittinen infrastruktuuri

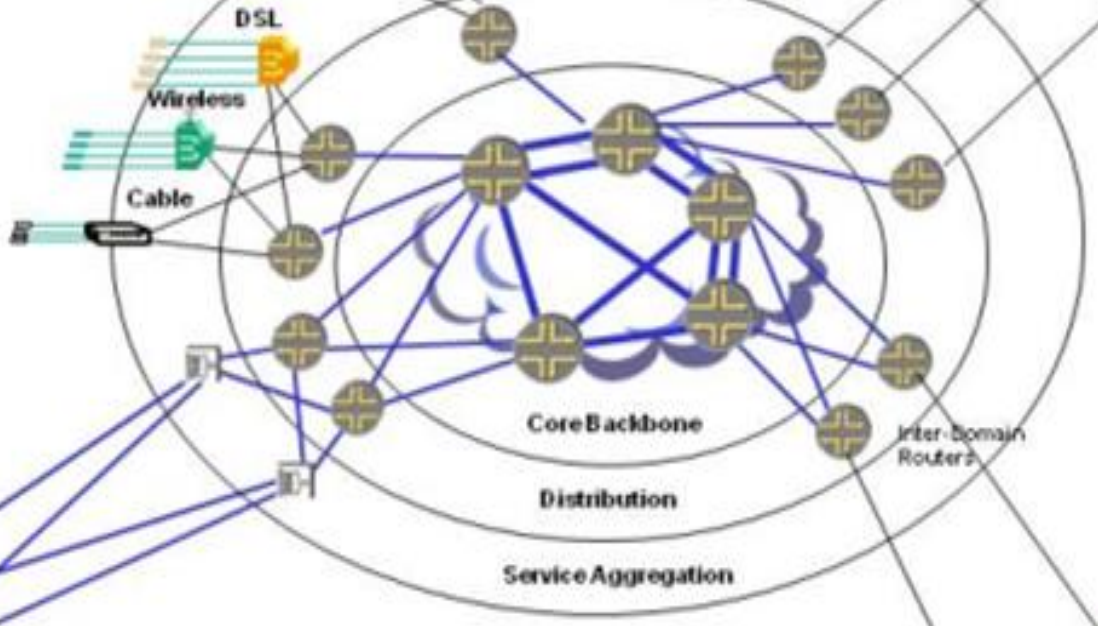
.mil

.gov

Julkishallinnon verkot

Kansalaiset verkossa

.fi



Elinkeinoelämän verkot

.com

Kriittinen informaatio-infrastruktuuri

Autonomiset järjestelmät ja robotiikka

Autonomiset älykkäät järjestelmät muuttavat niin taistelukentän kuin teollisuuden, työympäristön, sairaalan ja kodin.

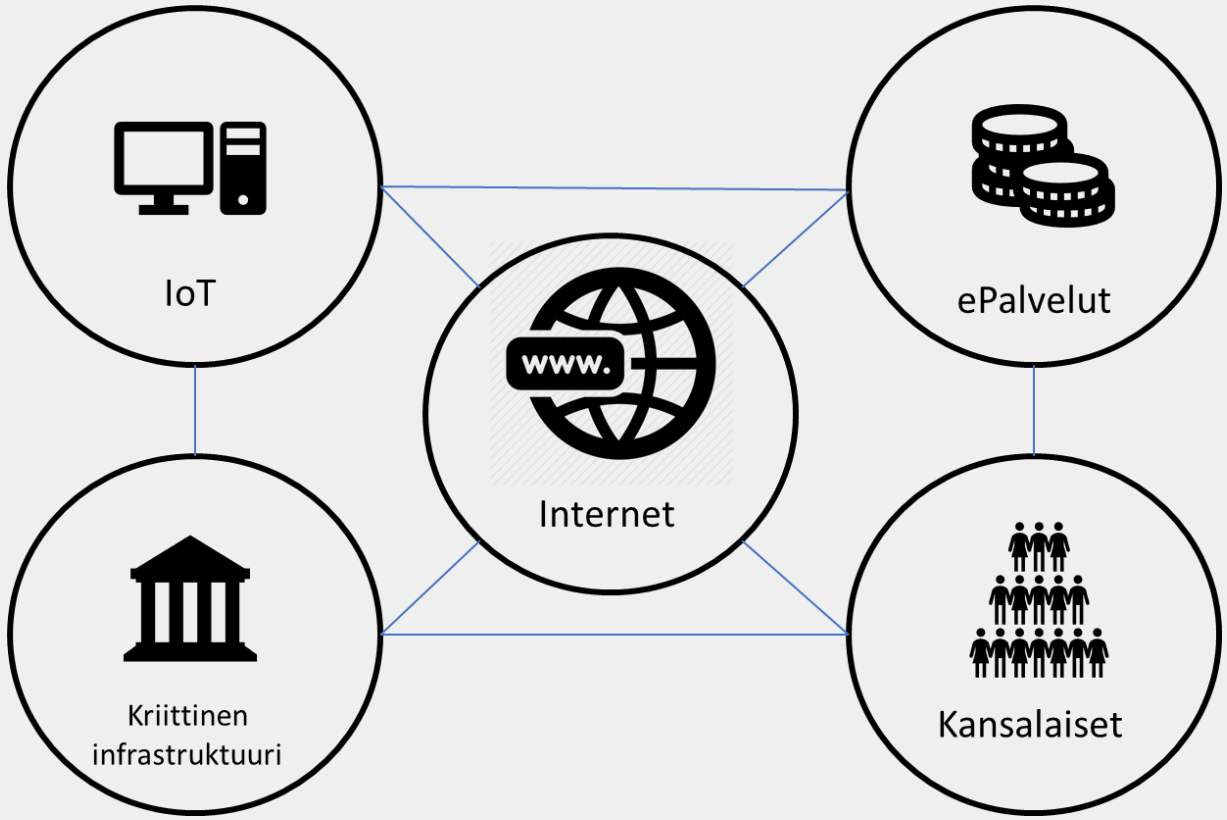
Tämä lisää mahdollisuuksia kyberhyökkääjille saada järjestelmiä hallintaansa.

Kybermaailma 2019

2018 lopussa maailmassa n. 23,1 miljardia verkkoon kytkettyä laitetta. Vuonna 2025: yli 75 miljardia.

Matkapuhelinten käyttäjiä maailmassa on yli 4,68 miljardia (61,3 %).

Vuonna 2018 ladattiin 258.2 miljardia applikaatiota



Vuonna 1998 3,6 % maailman väestöstä käytti internettiä.
Nyt käyttäjiä on noin 4,176 miljardia (54,7 %).

Päivittäin maailmalla:
- Lähetetään yli 200 miljardia sähköpostiviestiä,
- Lähetetään yli 500 miljoonaa twiittiä
- Käytetään Googlen hakukonetta 3,5 miljardia kertaa.

Facebookissa on yli 2,27 miljardia käyttäjää

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 (13.8.2018), 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.

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
Facebook	Renren	Vkontakte, Odnoklassniki
Gmail/Hotmail/Yahoo	QQMail/AliMail	Mail.ru
Internet	China Net	RuNet

Kyber-maailma 2025?

Esityksen sisältö

1 Digitaalisen maailman muutos

2 Kybermaailman uhkia

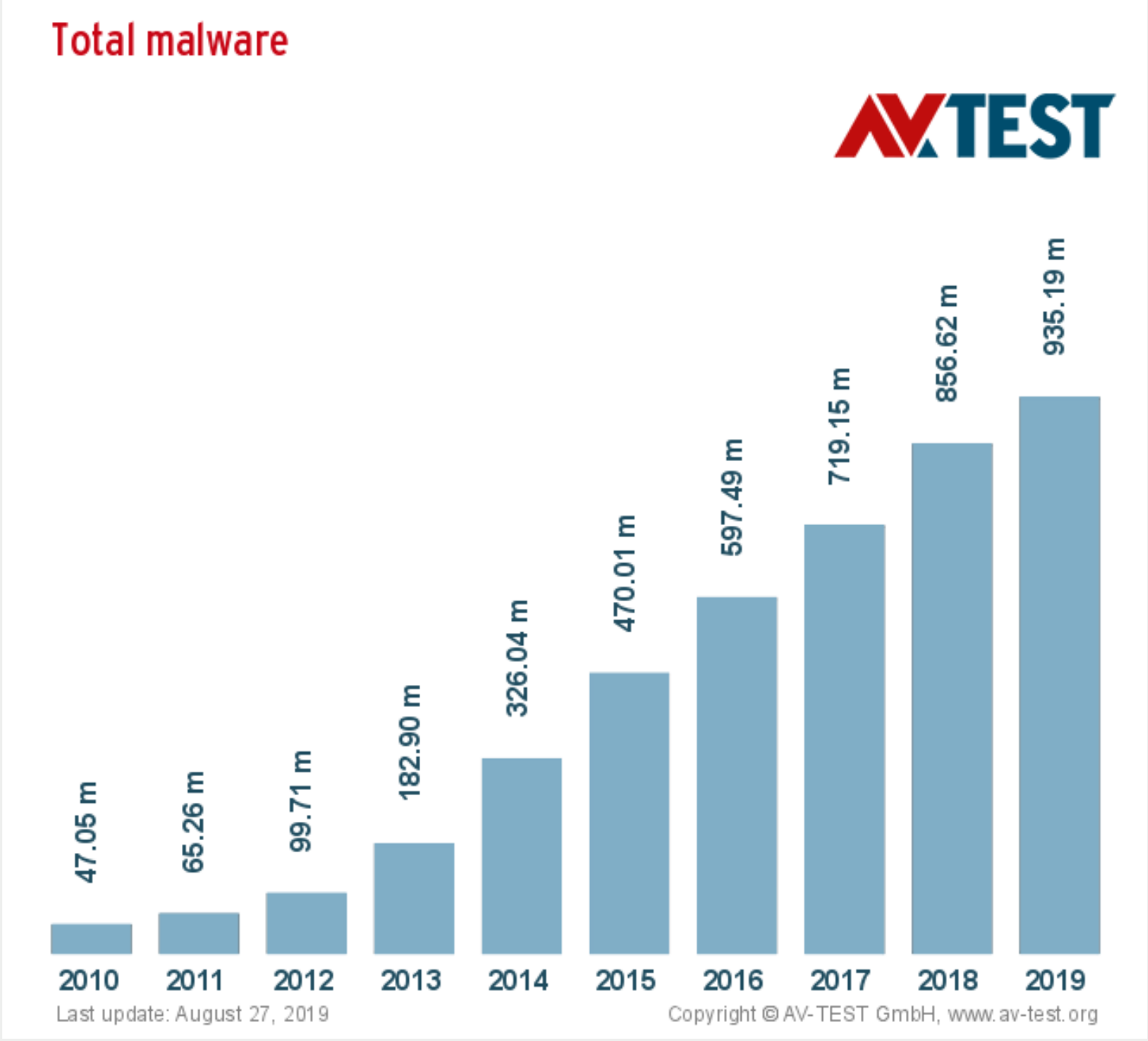
3 Kybermaailman haavoittuvuuksia

4 Kybermaailma ja ihminen

5 Turvallisuuden rakentaminen

Mega-tietomurrot

- Yahoo: 500 miljoonaa käyttäjätietoa, 3 Mrd.?
- Marriot: 500 miljoonaa asiakastietoa
- Friend Finder Network: 412 miljoonaa käyttäjätietoa
- Exactis: 340 miljoonan ihmisen henkilötietoja
- Equifax: 143 miljoonaa käyttäjätietoa
- Anthem: 78 miljoonaa potilastietoa
- Target: 70 miljoonaa asiakastietoa
- Ashley Madison: 32 miljoonaa asiakastietoa
- US Office of Personnel Management: 22 miljoonaa henkilötietoa
- US T-Mobile: 15 miljoonaa asiakastietoa

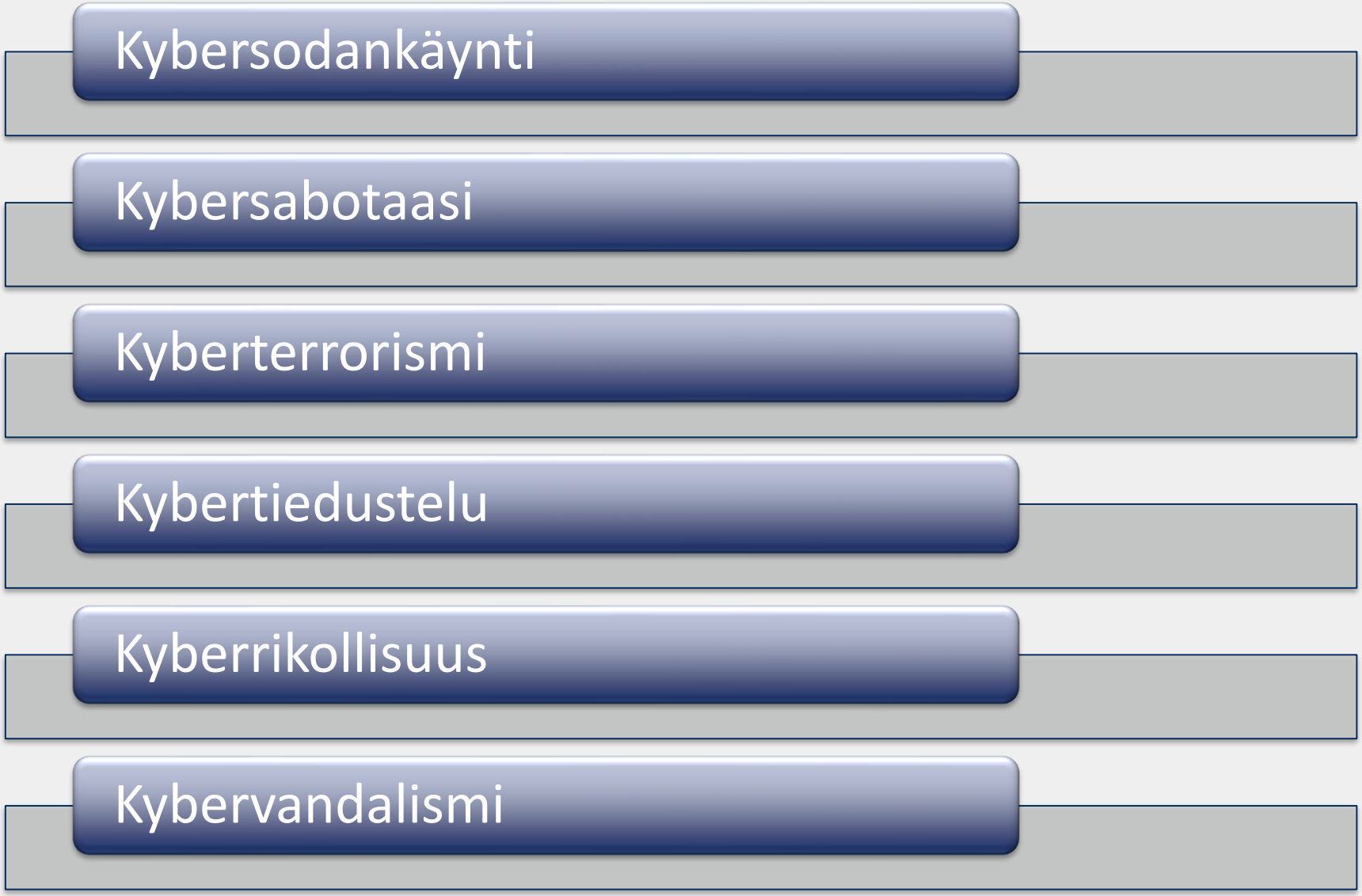


Haittaohjelma-tuotanto

350 000 uutta haittaohjelmaa joka päivä

Source: https://www.av-test.org/en/statistics/malware/

Kyberuhkamalli



Motivaatio ratkaisee

Kybervandalismi

Anarkiaan, kaaokseen ja haitantekoon tähtäävää toimintaa.

- Internet vahvisteinen: internetiä käytetään ylimääräisenä kommunikaatiokanavana
- Internet perustainen: internet toiminnan kohde

Kyberrikollisuus

Kyberrikoksia ovat rikokset, jotka ”tehdään sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen tai jotka kohdistuvat mainittuihin verkkoihin ja järjestelmiin".

Tietoverkkorikollisuus voidaan jakaa kolmeen alaryhmään:

1. Perinteiset rikollisuuden muodot, jotka on tehty käyttäen hyväksi viestintäverkkoja ja tietojärjestelmiä.
2. Laittoman sisällön julkaiseminen sähköisissä viestimissä.
3. Rikokset, joita esiintyy ainoastaan sähköisissä verkoissa, kuten hyökkäykset tietoverkkoa vastaan, palvelunesto tai hakkerointi.

Attribuutio-ongelma
Rajattomuus

Menetykset globaalisti $ 400+ miljardia (USA 50-100 Mrd. $)

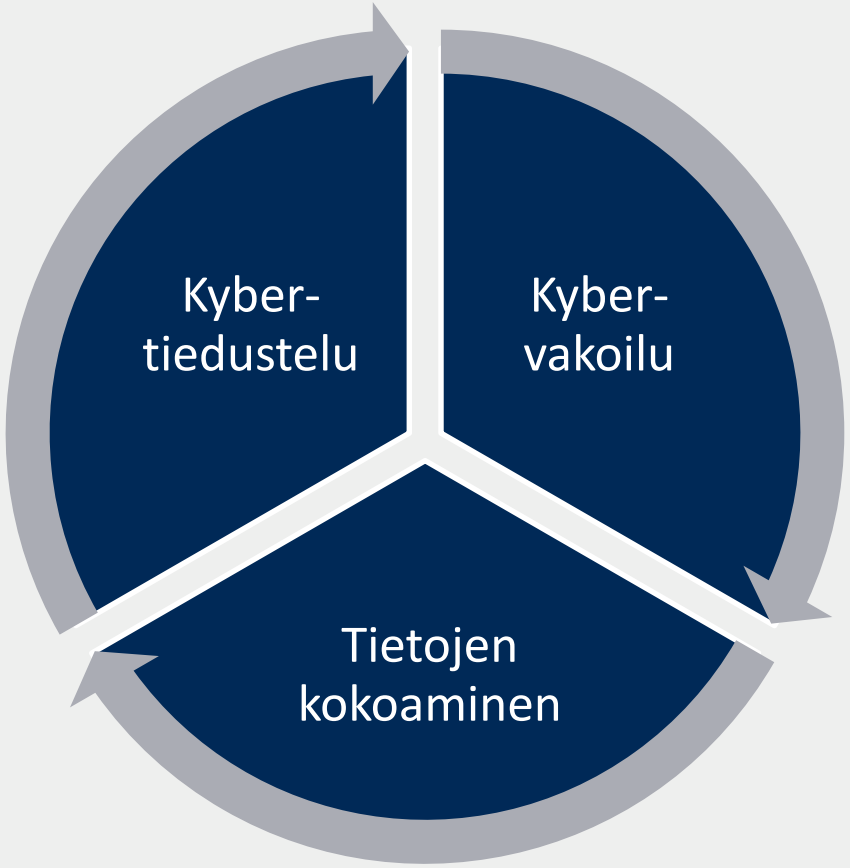
Kyberrikollisuuden palveluhinnasto

- Facebook tai Twitter tilin hakkerointi: $130
- Gmail hakkerointi: $162
- Organisaation postilaatikon hakkerointi: $500
- Windows rootkit asennus: $292
- Winlocker kiristysohjelma: $10-20
- Verkkoliikenteen seuranta: $7-15 per 1,000 käyttäjää
- Haittaohjelman asentaminen tiedostoon: $10-30
- Palvelunestohyökkäyksen (DDoS) vuokra: $30-70 päivässä, $1,200 kuukaudeksi
- Email spam: $10 per miljoona e-mails
- SMS spam: $3-150 per 100-100,000 viestiä
- Bot-verkon luominen: $200 per 2,000 botin verkko
- DDoS botverkko: $700
- ZeuS lähdekoodi: $200-$500

Lähteet: Ars Technica, Wired, Russian Underground 101, Trend Micro, Max Goncharov

Kybertiedustelu-vakoilu-tiedon kokoaminen

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.



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.

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.

Kevyt valvontalennokki

Snoopy voi seurata WiFi-signaaleita, RFID-signaaleja sekä Bluetooth- ja PAN/WPAN-liikennettä (IEEE 802.15).

Yhdessä GPS-vastaanottimen kanssa se voi paikantaa signaalilähteet ja siten seurata puhelimia, tablet-laitteita, tietokoneita, ja myös sydämentahdistimia, älyrannekkeita, älykelloja.

ArsTechnica, Dan Goodin - Mar 26 2014

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.

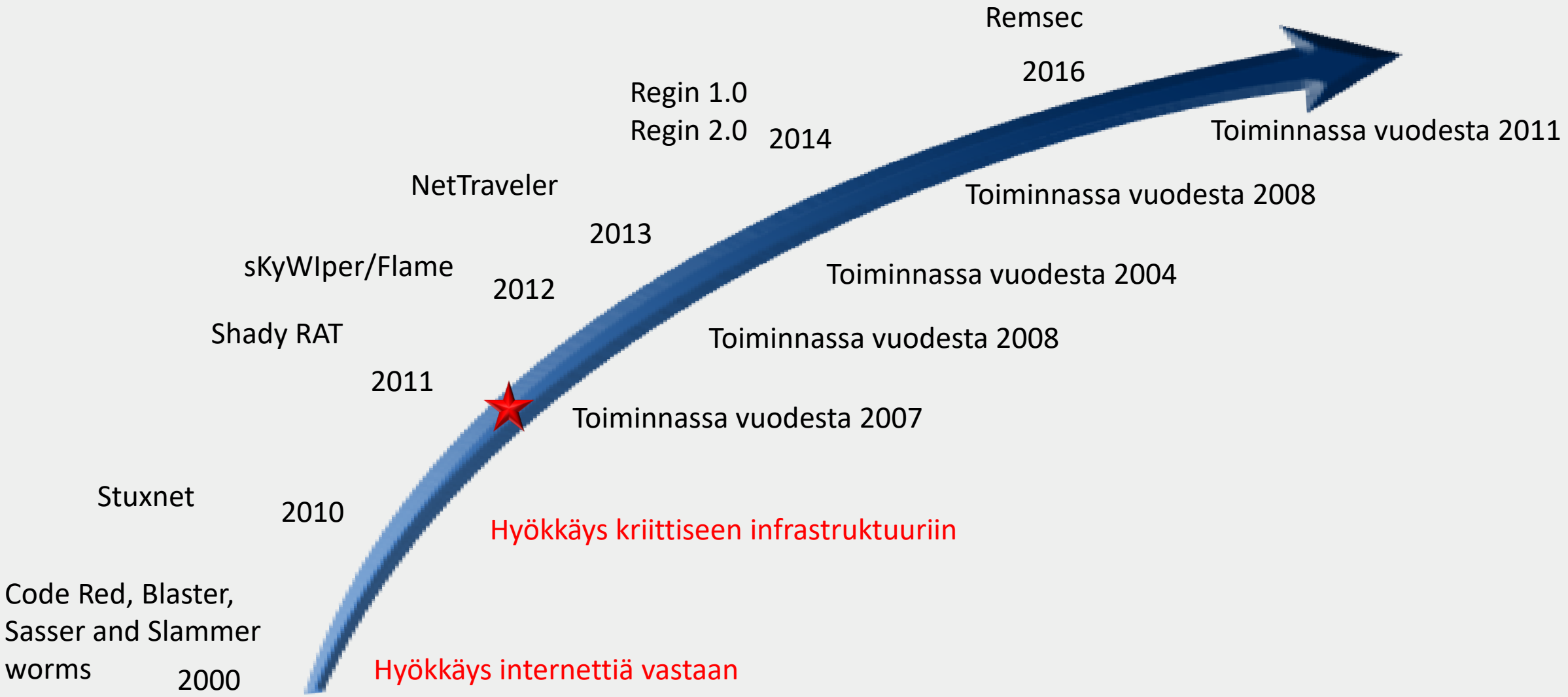
12.9.2019

Matkapuhelin hyökkäyskohteena

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.

Kyberoperaatioiden havaittavuus



Kyberterrorismi

Kyberterrorismissa käytetään tietoverkkoja hyökkäyksiin kriittisiä informaatiojärjestelmiä kohtaan ja niiden kontrollointiin. Hyökkäysten tavoitteena on tuottaa vahinkoa ja levittää pelkoa ihmisten keskuuteen.

> The Islamic State terrorist organization appears eager to enter into digital jihad, boasting of plans to establish a “cyber caliphate” from which to mount catastrophic hacking and virus attacks on the United States and the West.

Kybersabotaasi

Stuxnet on Windows-spesifinen tietokonemato, joka vakoilee ja uudelleenohjelmoi teollisuusjärjestelmiä.

Mato oli päässyt Iranin ydinlaitoksiin saastuneessa USB-muistitikussa.

Mato hyökkäsi Windows-käyttöjärjestelmää vastaan hyödyntäen neljää haavoittuvuutta, joista kaksi oli ennalta tuntemattomia ns. nollapäivähaavoittuvuuksia.

2010

Hyökkäys sähköverkkoon

Laaja sähköverkon lamautus kyberhyökkäyksellä joulukuussa 2015

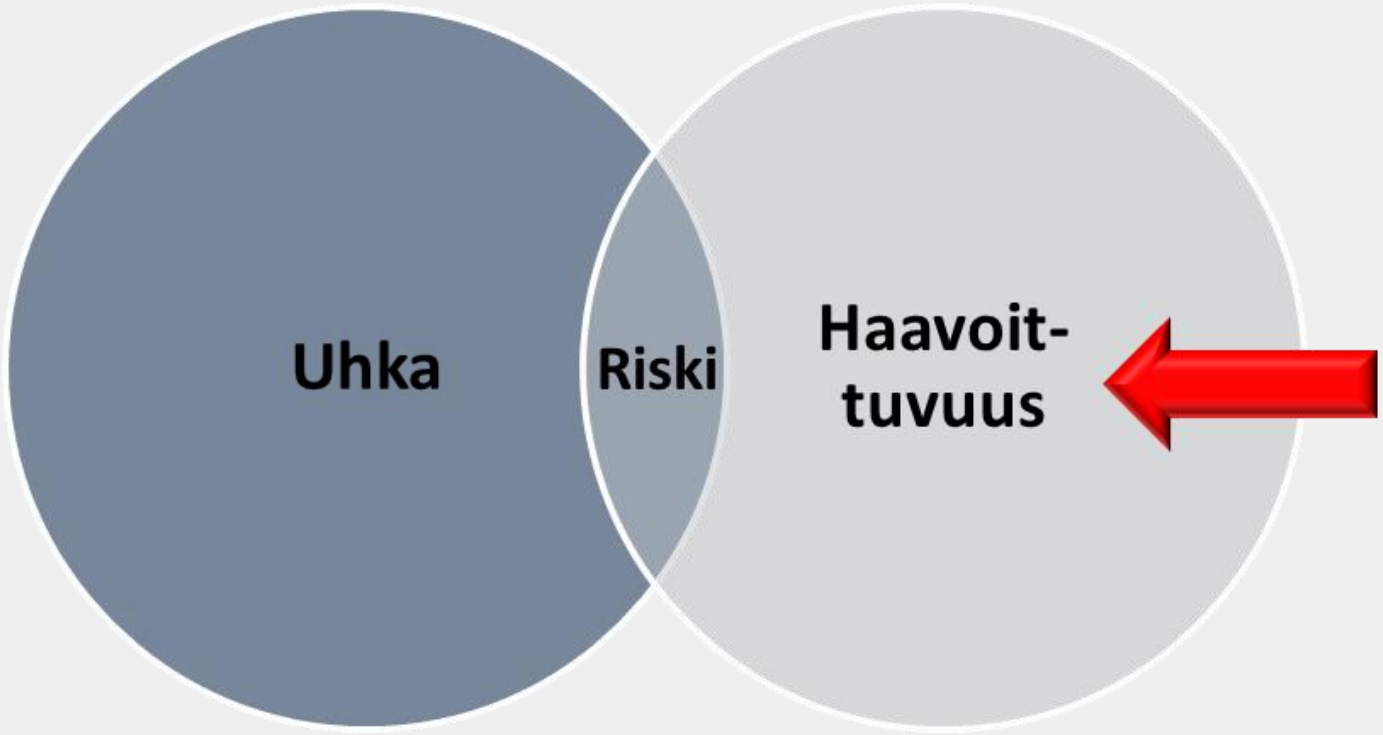
Ukrainalaisen sähköyhtiön 80 000 asiakkaalta onnistuttiin katkaisemaan sähkönsaanti kuudeksi tunniksi. Itse sähkönjakeluun päästiin käsiksi yhtiön työasemiin ja palvelimiin istutetulla haittaohjelmalla. Tilannetta pyrittiin lisäksi hämmentämään pommittamalla energiayhtiön asiakaspalvelua häirintäsoitoilla, jolloin asiakkaiden vikailmoitukset eivät päässeet läpi.

Kybersodankäynti

Kybersodankäynti on osa sodan voittamiseen tähtääviä operaatioita.

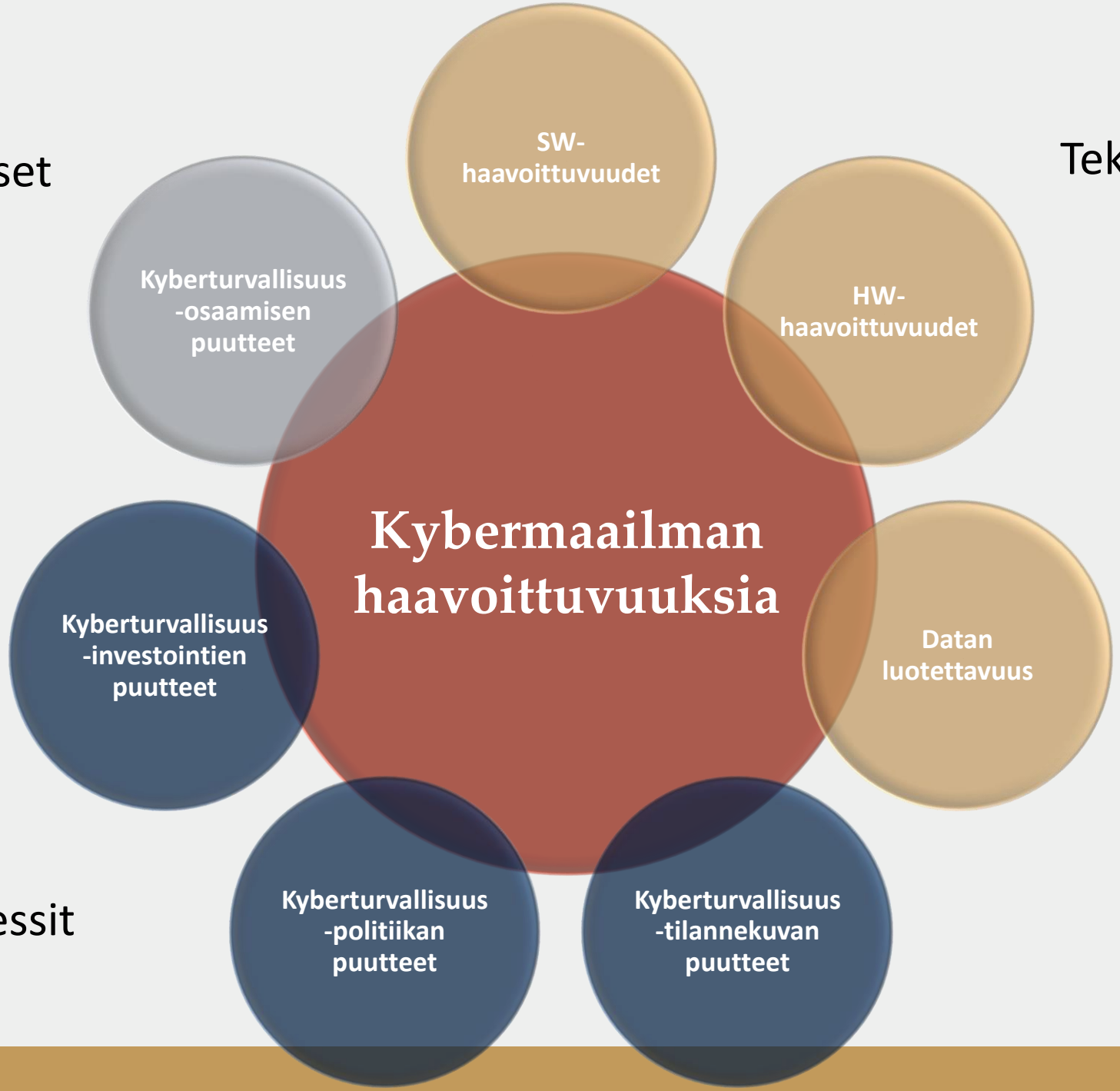
Esityksen sisältö

Uhka + haavoittuvuus = riski



Ihmiset

Teknologia



Prosessit

Kybermaailman haavoittuvuuksia

SW-haavoittuvuuksia

DIGI & TEKNIIKKA

Digi & tekniikka | Digiuutiset

Facebookin ohjelmistovirhe muutti miljoonien käyttäjien yksityisyysasetuksia

08.06.2018 klo 1:50

Ohjelmistovirhe aiheutti sen, että käyttäjien ystäville tarkoitetut julkaisut saattoivat näkyä julkisina.

UUTISET Tuoreimmat Urheilu Sää | Kotimaa Ulkomaat Talous Politiikka Kulttuuri Kolumnit Lu

Washington Post: Boeing 737 Max -konemallissa on toinenkin ohjelmisto-ongelma

Boeingin mukaan kyseessä on melko pieni ongelma.

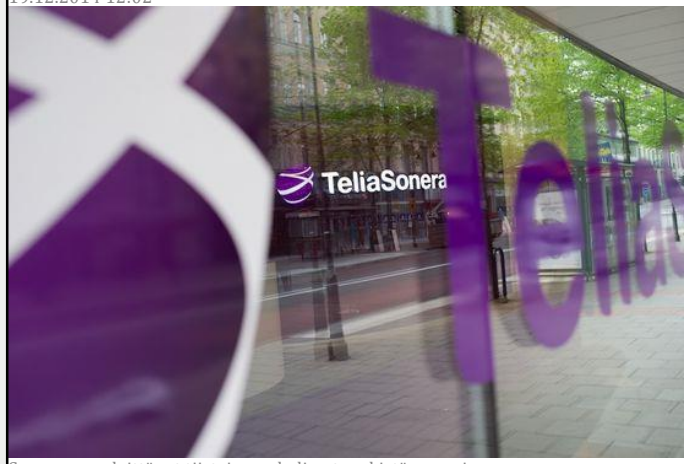
Boeing 737 MAX 5.4.2019 klo 05.42

SW-haavoittuvuuksia

Ohjelmistovirhe mykisti puhelimet

US

Uusi Suomi
Luotu:
19.12.2014 12:02



Sonera on selvittänyt tiistaina puhelimet mykistäneen vian syyn.

KOTIMAA
Soneran viime tiistainen vika johtui päivitystyön yhteydessä paljastuneesta ohjelmistovirheestä.

Soneran puheyhteydessä ja tekstiviestipalvelussa oli tiistaiaamuna valtakunnallinen vika. Vika alkoi noin kello 10 ja päättyi noin 11.30. Vika vaikutti erityisesti Soneran 2G- ja 3G-verkkojen puheyhteyteen. Myös tekstiviesteissä oli ongelmia. Data toimi normaalisti 4G-verkossa.

Soneran mukaan ennalta suunniteltu ja testiympäristössä onnistunut muutostyö laukaisi tuotantoon viennin jälkeen piilevän ohjelmistovirheen signalointiyksiköissä. Tämän seurauksena signalointiyksiköt kaatuivat.

Tässä lentokonemallissa on melko ikävä ohjelmistovirhe - "Saattaa sulkea itsensä yllättäen, myös koneen ollessa ilmassa"

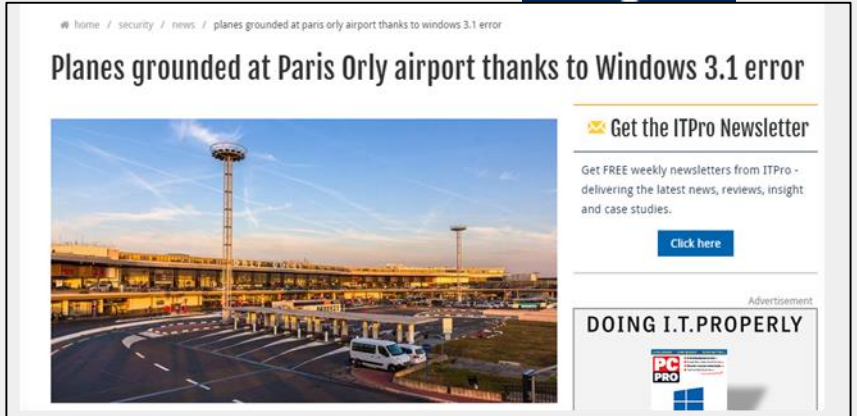
Talouselämä 4.5.2015 21:21päivitetty 27.8.2015 06:12

Boeing 787 -mallin lentokone

Yhdysvaltain ilmailuviranomaiset ovat antaneet uuden ohjeistuksen koskien Boeing 787 -malleja. Koneiden sähkövirtaa tuottavan generaattorin ohjausyksikkö saattaa sulkea itsensä yllättäen, myös koneen ollessa ilmassa.

Ohjausyksikön ohjelmisto ei toimi yhtäjaksoisesti yli 248 päivää. Mikäli aika ylittyy, generaattori menee vikasietotilaan, FAA varoittaa.

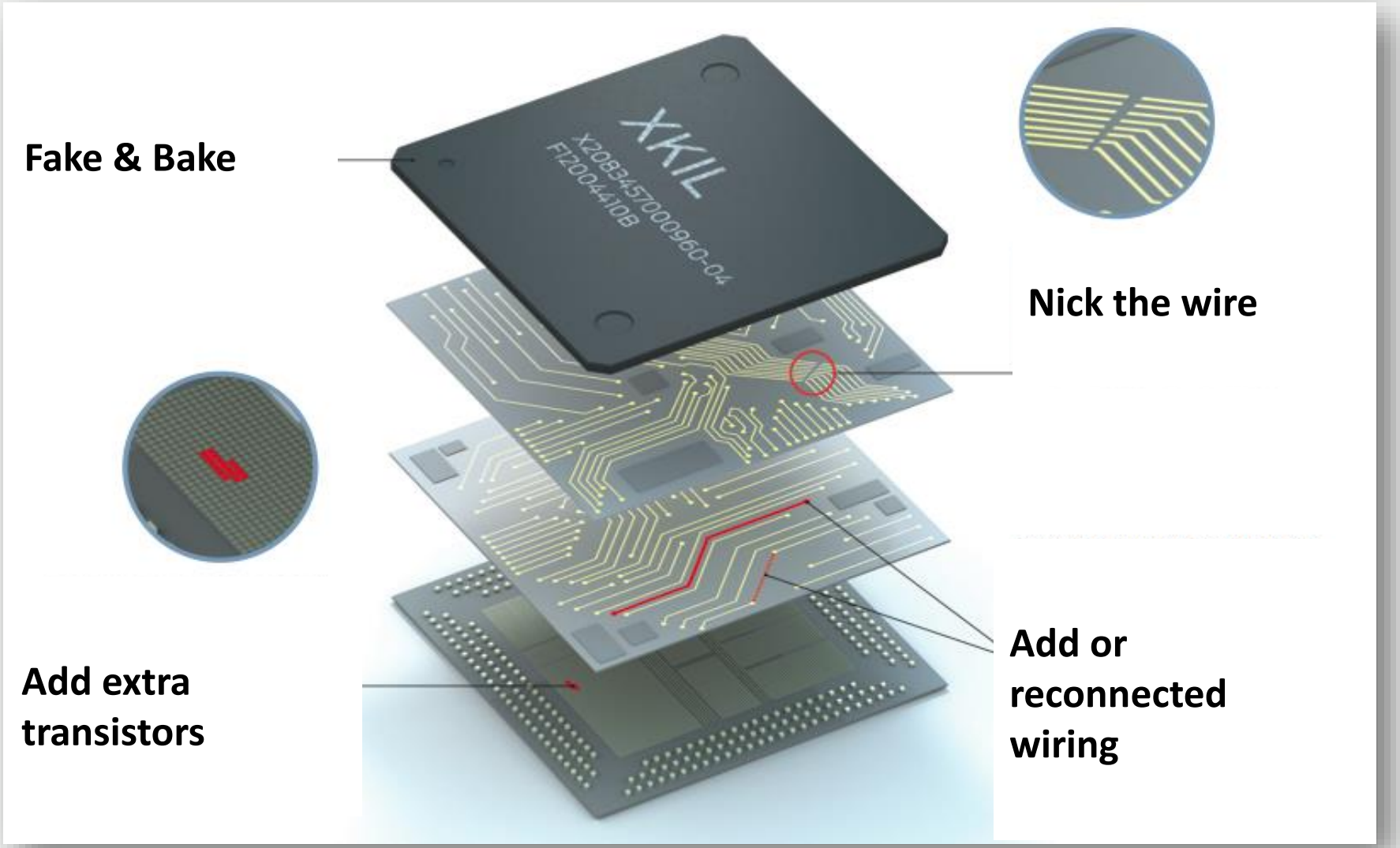
Pahimmillaan kaikki generaattorit olisi käynnistetty samanaikaisesti, ja ne sammuisivat yhtä aikaa, The Register kirjoittaa.



Pariisin lentoasema jouduttiin sulkemaan, kun Windows 3.1 – käyttöjärjestelmä kaatui.

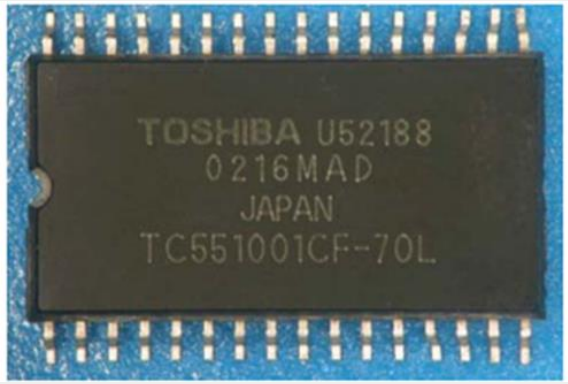
7.11.2015

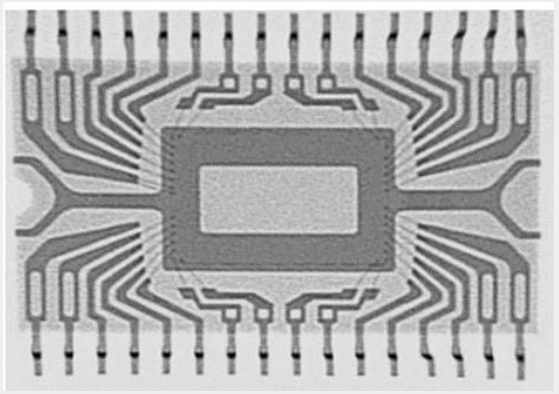
HW-haavoittuvuuksia



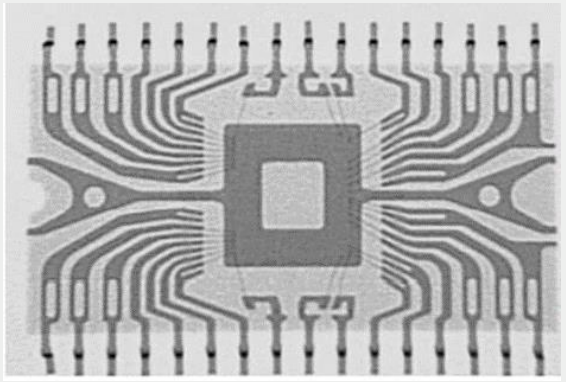
Source : Thehuntforthekillswitch.http://www.spectrum.ieee.org/semiconductors/ design/the-hunt-for-the-kill-switch.

HW-haavoittuvuuksia
Component corruption

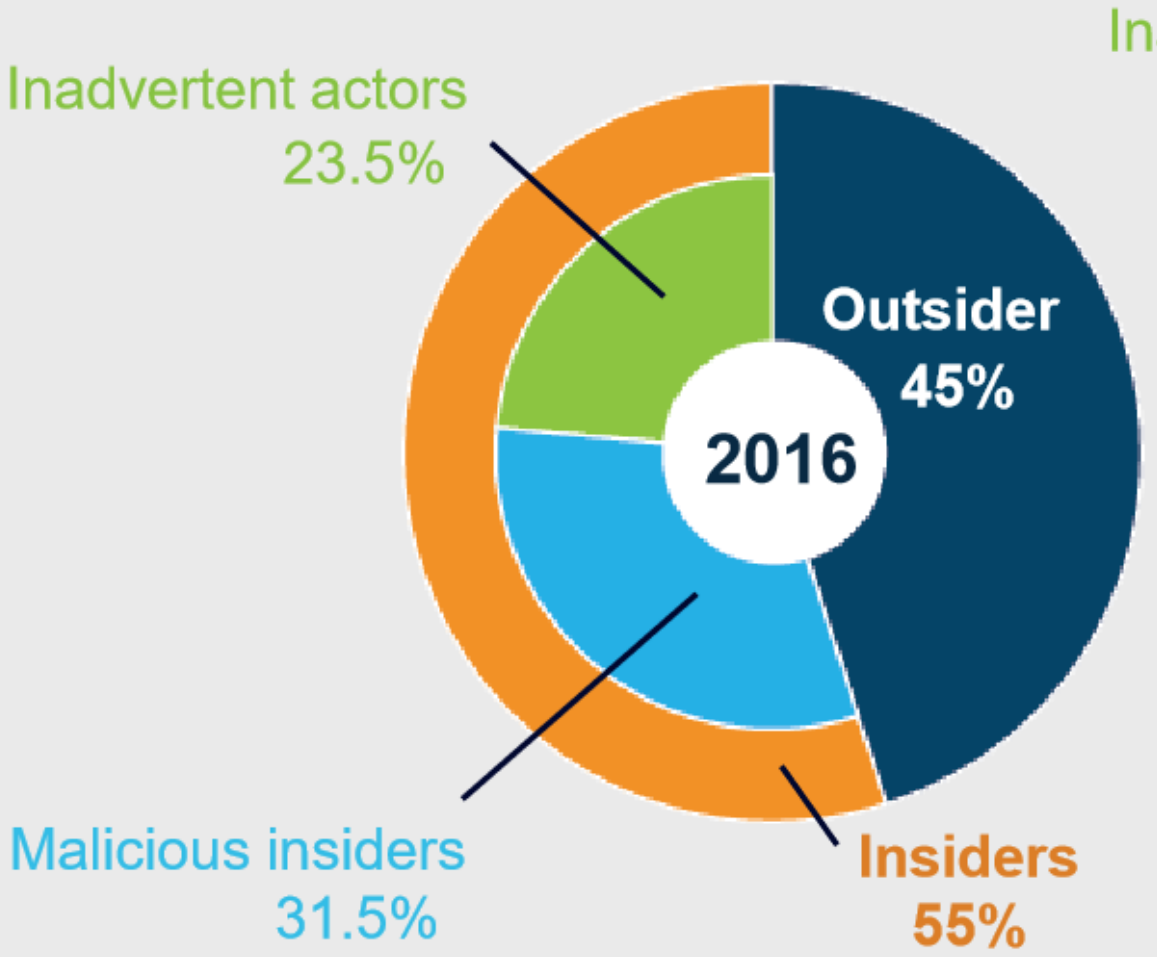


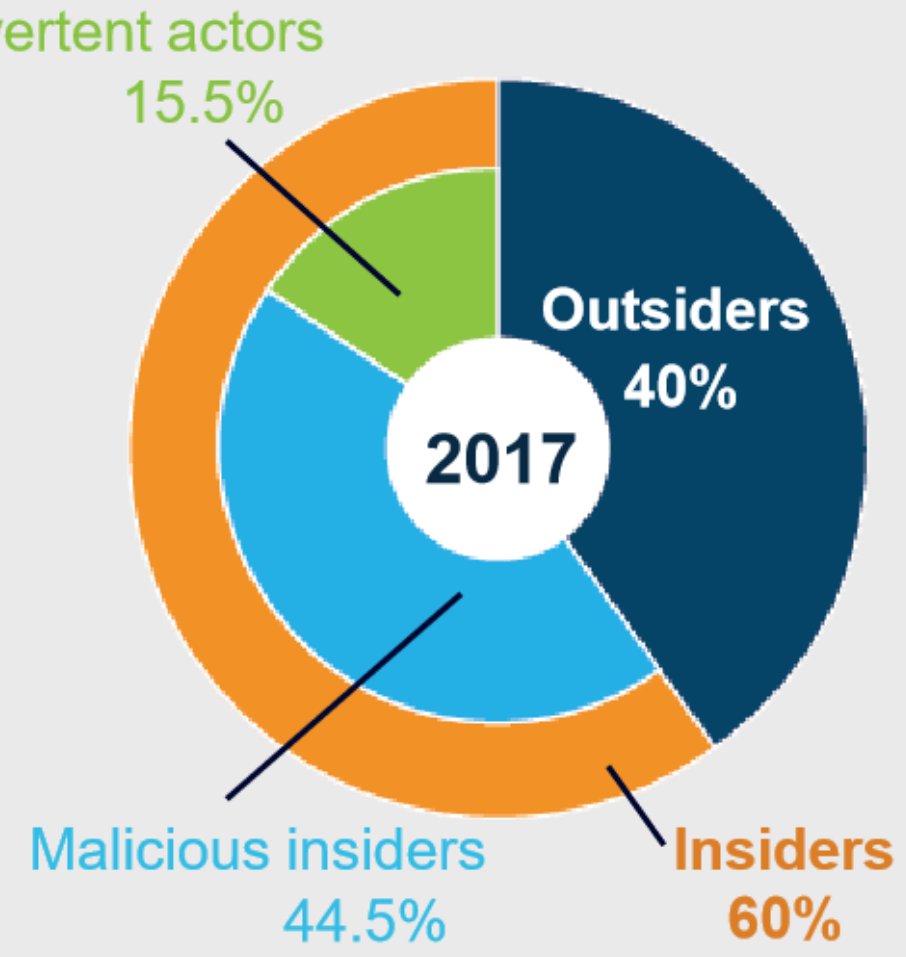


Röntgenkuvaus



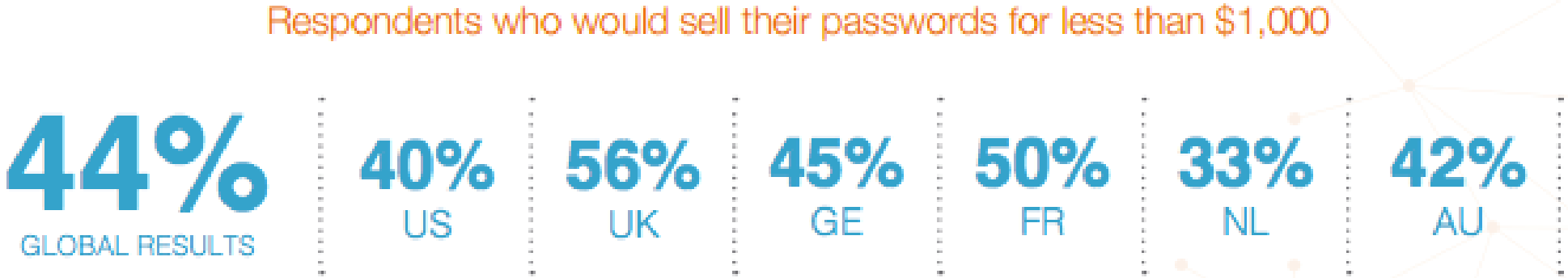
Sisäiset vs. ulkoiset uhat





Source: IBM Think 2018

Inhimilliset riskit



Esityksen sisältö

Kansalainen ja tiedon kokoaminen

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

Sijainti

Google Maps näyttää nyt sijaintisi muille

Google Maps -palvelu saa uuden ominaisuuden: sijainnin jakamisen. Käyttäjä voi jakaa reaaliaikaisesti oman sijaintinsa haluamilleen henkilöille, kuten ystäville tai perheenjäsenille.

Google Earth on karttapalvelu, joka yhdistää satelliitti- ja ilmakuvia sekä paikkatietoja muodostaen kolmiulotteisen kuvan.

Google Earthin alkuperäinen nimi oli Earth Viewer, jonka kehitti Keyhole, Inc.

Google osti ohjelman 2004 ja siitä muodostui Google Earth 2005.

Sopimus, jonka olet tehnyt

Sisältösi Google Mapsissa ja Google Earthissa. Google Mapsiin tai Google Earthiin lähettämääsi, lataamalla lähettämääsi tai tallentaamasi tai niistä vastaanottamaasi Sisältöä valvotaan Googlen Yleisten käyttöehtojen mukaisesti, osiossa "**Sisältösi Palveluissamme"** eritellyt käyttöoikeudet mukaan lukien.

Kun lataat, lähetät tai tallennat sisältöä Palveluihin tai niiden kautta tai vastaanotat sisältöä Palveluista tai niiden kautta, **annat Googlelle (ja yhteistyökumppaneillemme) maailmanlaajuisen oikeuden käyttää, ylläpitää, tallentaa, jäljentää, muokata, välittää, julkaista, esittää ja levittää kyseistä sisältöä, asettaa sitä julkisesti esille sekä luoda siitä johdannaisteoksia (esimerkiksi teoksia, jotka syntyvät kääntämällä, sovittamalla tai tekemällä teokseen muita muutoksia, joiden avulla sisältö saadaan toimimaan Palveluissa paremmin).**
Tämä käyttöoikeus on tarkoitettu yksinomaan Palveluiden ylläpitämiseksi, markkinoimiseksi ja parantamiseksi sekä uusien palveluiden kehittämiseksi.
Tämä käyttöoikeus pysyy voimassa vaikka lopettaisit Palveluiden käytön, ja se koskee esimerkiksi yritystietoja, jotka olet lisännyt Google Mapsiin.

Älypuhelimesta seurantalaite

Tietoja kuluttajien sijainnista kerääviä majakoita on maailmassa 8 miljoonaa. Vuonna 2020 niitä on jo puoli miljardia.

Majakoita asennetaan parhaillaan 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 Instagramin, AirBnb:n tai Facebookin kaltaisen sovelluksen, joudut hyväksymään käyttöehdot ja sallit paikantamisen.

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.
Hei väittävät, että nämä puutteet heikentävät kyberturvallisuutta ryhmäkeskusteluissa.

Kasvojen tunnistuksesta tunteiden tunnistukseen

Automaattinen kasvojen tunnistus ihmismassojen skannaamisen.

Facebook käyttää palvelussaan automaattista kasvojen tunnistusta.

Windows 10 sisältää Windows Hello -palvelu: tietokoneelle tunnistautuminen kasvojen tunnistusta käyttämällä.

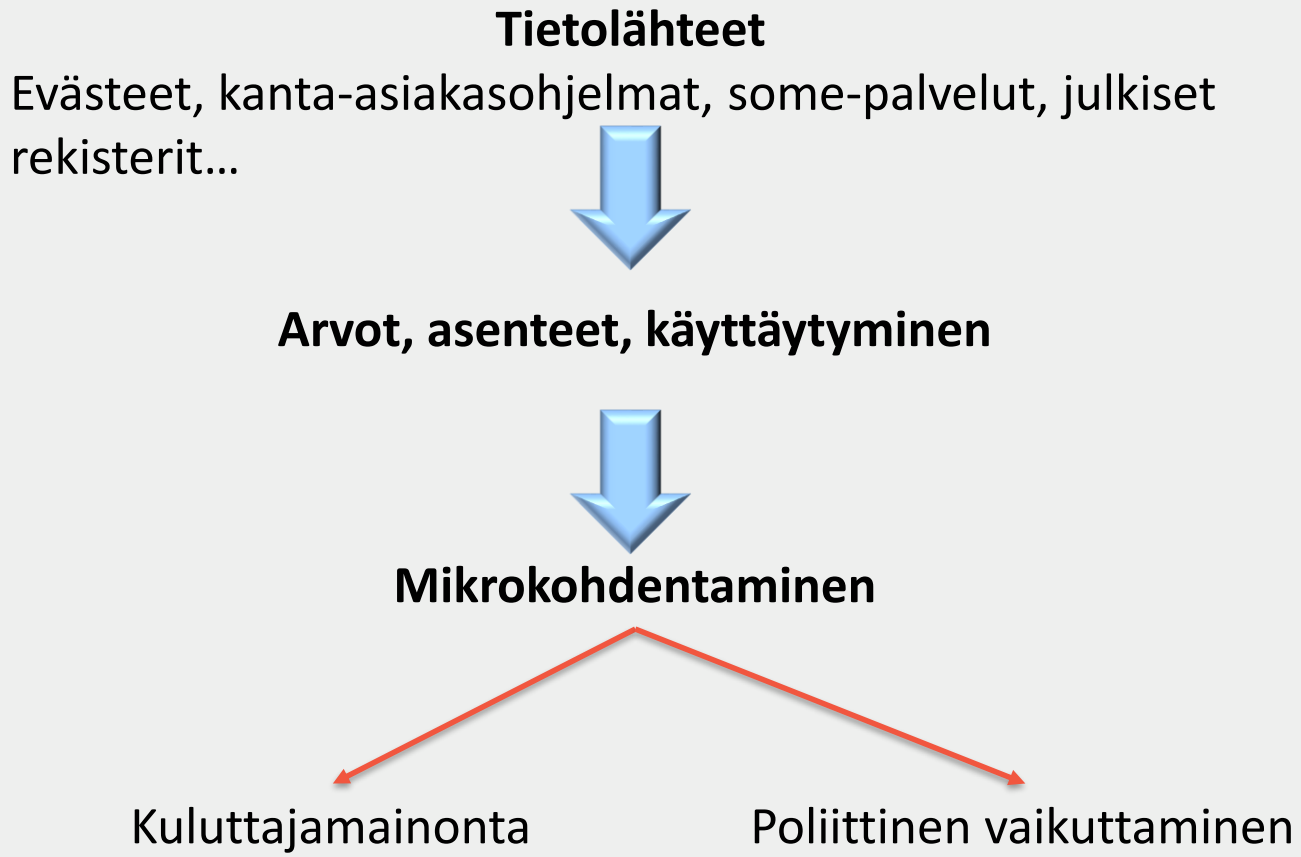
Yksilön tunnistaminen

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

Persoonallisuuden tunnistaminen

Henkilötiedot analyysin kohteena: Psychographics

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



Henkilötiedot analyysin kohteena

Facebook: Jopa 2,7 miljoonan eurooppalaisen tiedot annettu Cambridge Analyticalle.

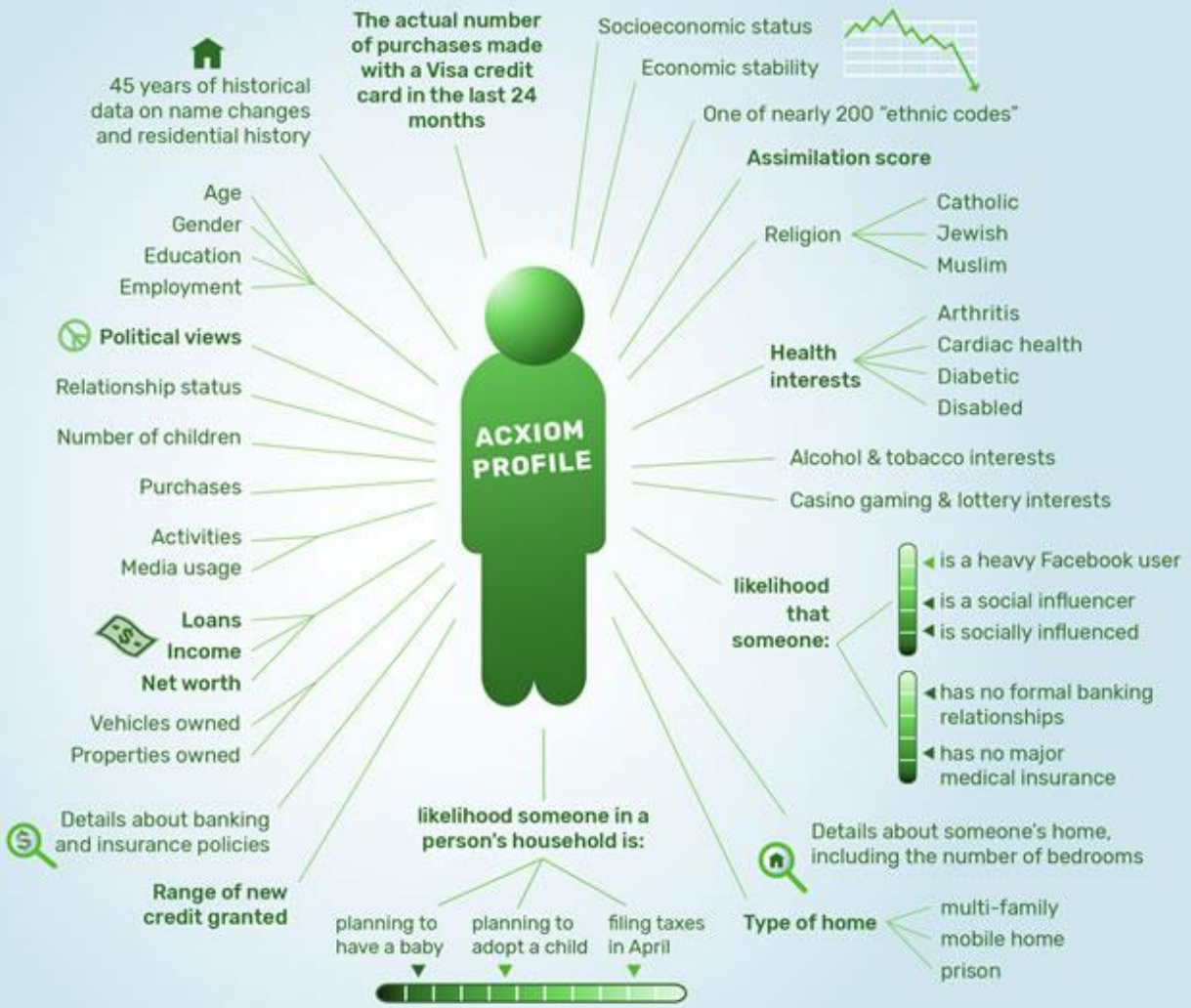
YLE 6.4.2018

Sosiaalisen median palvelu Facebook neuvotteli useiden amerikkalaissairaaloiden kanssa niiden potilastietojen käyttämisestä tutkimusprojektiinsa. Yhtiön tarkoituksena oli yhdistää saamansa potilastiedot itse käyttäjistään keräämän datan kanssa ja tutkia, voisiko se auttaa sairaaloita löytämään helpommin hoitoa kaipaavia ihmisiä.

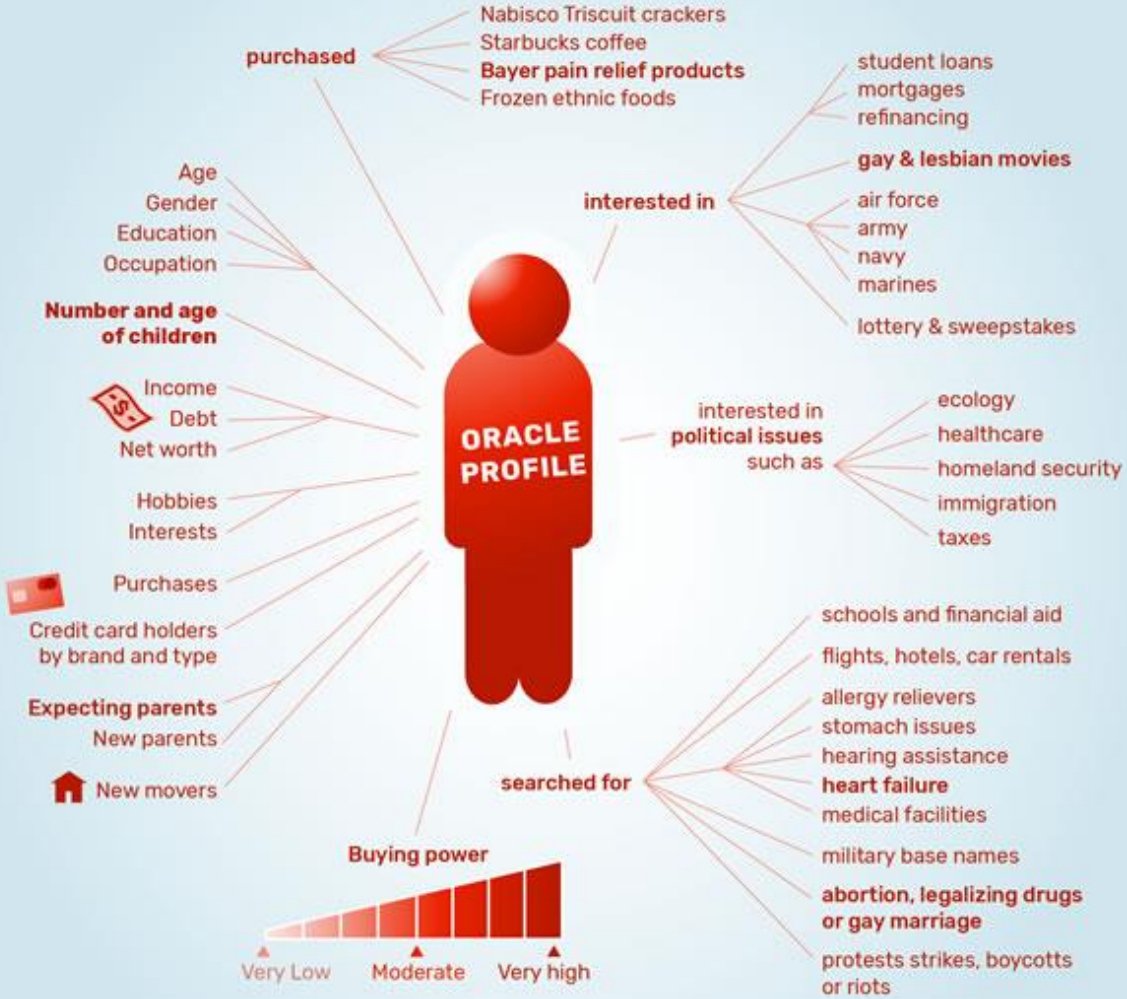
CNBC 5.4.2018

DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

Examples of data on consumers provided by Acxiom and Oracle



Acxiom provides of up 3,000 attributes and scores
on 700 million people in the US, Europe, and other regions.



Oracle sorts people into thousands of categories
and provides > 30,000 attributes on 2 billion consumer profiles

Esityksen sisältö

1 Digitaalisen maailman muutos

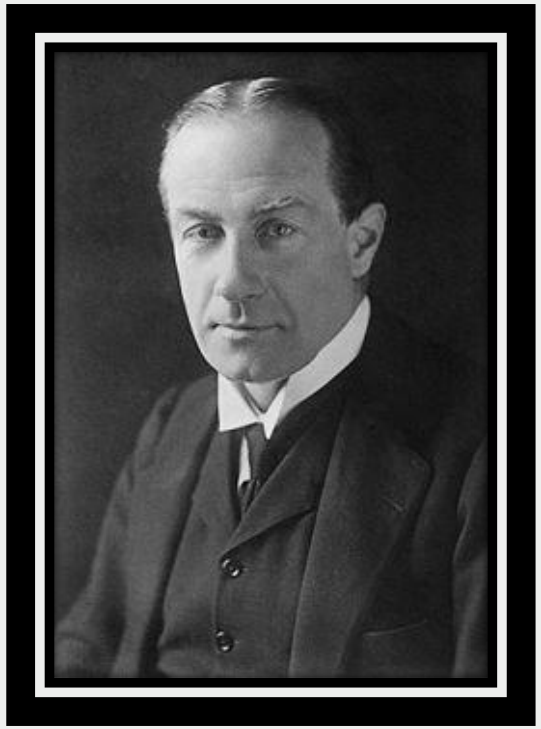
2 Kybermaailman uhkia

3 Kybermaailman haavoittuvuuksia

4 Kybermaailma ja ihminen

5 Turvallisuuden rakentaminen

”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

Uhka + Haavoittuvuus → Riskin arvo → Vastatoimenpiteet

- Kyber-vandalismi
- Kyber-rikollisuus
- Kybervakoilu
- Kyber-terrorismi
- Kyber-sabotaasi
- Kyber-sodankäynti

- Ihmiset
- Prosessit
- Teknologia

- Liike-toiminta, IPR
- Maine
- Oikeudel-linen, GDPR
- Palautus ja korjaus

Johtaminen
- Toimintaohjeet/politiikka
- Implementaatio
- Osaamisen hallinta

Kyberkulttuuri
- Sääntely
- Yhteisön arvot ja normit
- Yhteisöllisyys

Järjestelmähallinta
- Riskien hallinta
- Suojausteknologiat
- Resilienssi


Identiteettianalyysi
- SoMe ympäristö
- Peliympäristö
- Palveluympäristö
Kuka sinä olet?
Profilointi
- Palveluntarjoajat
- Yritykset ja yritysketjut
- Jäsenyydet
Mistä olet kiinnostunut?
Seuranta
- Älypuhelin
- Tietokoneet, tabletit
- Navigaattori
Missä sinä olet?
Tiedonhankinta
- Henkilökohtaiset tiedot
- Henkilökohtainen viestintä
- Henkilötiedot eri rekistereissä
Mitä tietoja sinusta tai sinulla?
Uhat yksityisyyttä vastaan

Henkilökohtainen kyberturvallisuus

1. Muista nettipalveluihin liittyessäsi, ettei mikään ole oikeasti ilmaista
2. Pyri ymmärtämään palvelun käyttöehdot
3. Käytä kaikissa nettilaitteissa luotettavia suojausohjelmistoja ja hoida päivitykset
4. Kaikki nettiin laitettu on siellä ikuisesti – mieti mitä sinne tallennat
5. Kaikki salaus- ja rajoitusasetukset ovat murrettavissa – käytä kuitenkin hyvää salasanaa (salasana/palvelu), äläkä tallenna sitä selaimeen
6. Hoida raha-asioita vain oman tutun pankkisi kanssa
7. Älä ole yhteydessä tuntemattomiin netissä
8. Älä avaa epäilyttäviä posteja, erityisesti liitetiedostoja
9. Älä liitä laitteisiisi muiden lisälaitteita (USB-tikku, irtokovalevy, nettikamera jne.)
10. Toteuta toimiva varmuuskopiointijärjestely
11. Se mikä tuntuu netissä tosi upealta on erittäin todennäköisesti huijausta
12. Kaikessa nettityöskentelyssä tarvitaan tervettä epäluuloa