JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Teollisuuden kyberturvallisuuden kestävyys

Tutkimusjohtaja, ST eversti evp. Martti Lehto

5.9.2024

Print subscriptions | Sign in | Search jobs | Search | Europe edition

Support the Guardian

Fund independent journalism from €4 per month

Support us →

The Guardian

News | Opinion | Sport | Culture | Lifestyle | More

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

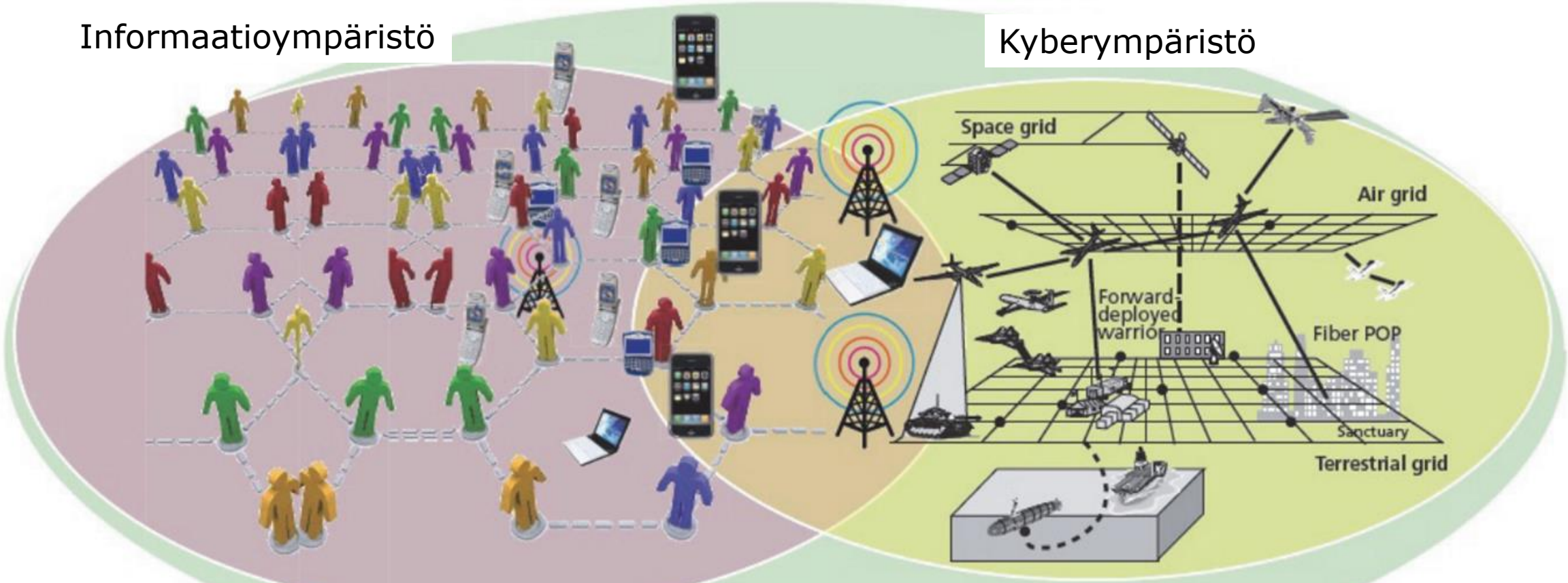
Chinese government-linked hackers have burrowed into US critical infrastructure and are waiting "for just the right moment to deal a devastating blow"

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

Esityksen sisältö

1. Kyber-fyysinen maailma
2. Haavoittuvuuksia kybermaailmassa
3. Kyberrikollisuudesta
4. Kybertiedustelusta
5. Kriittinen infrastruktuuri kohteena
6. Päätelmiä

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

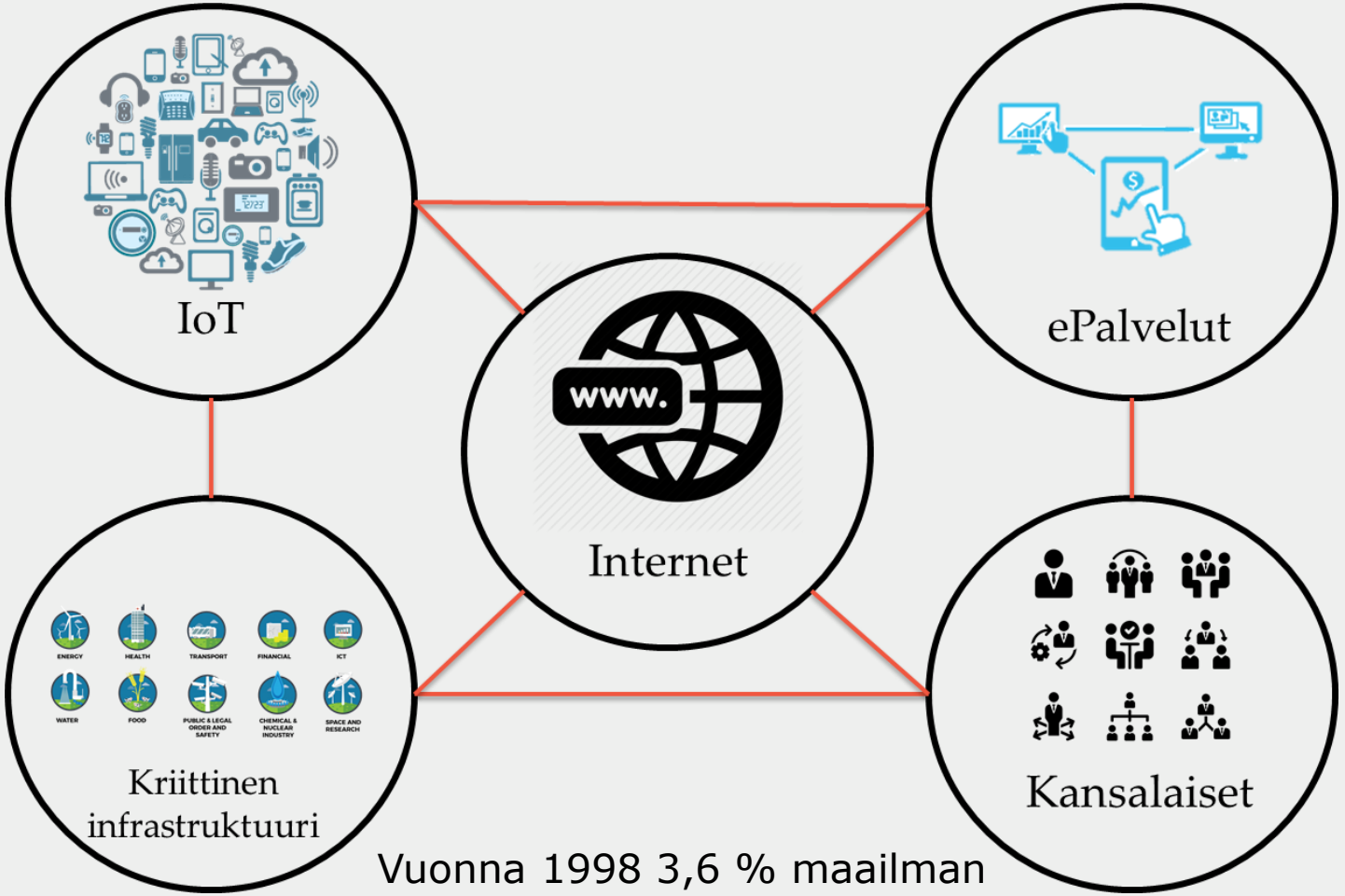
Digitaalinen kybermaailma 2024

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 2022 ladattiin noin 255 miljardia matkapuhelin applikaatiota.



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

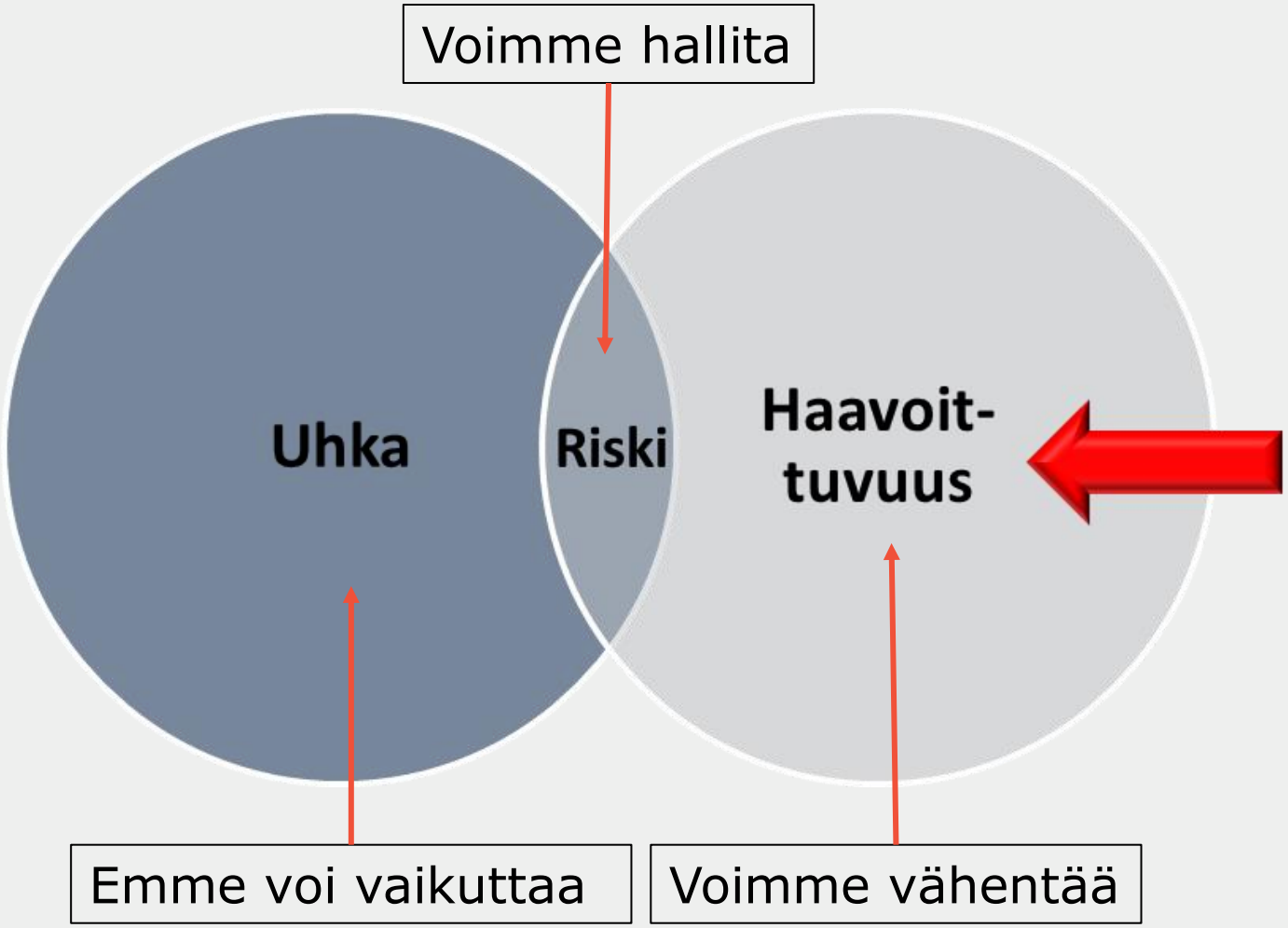
Päivittäin maailmalla:

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

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

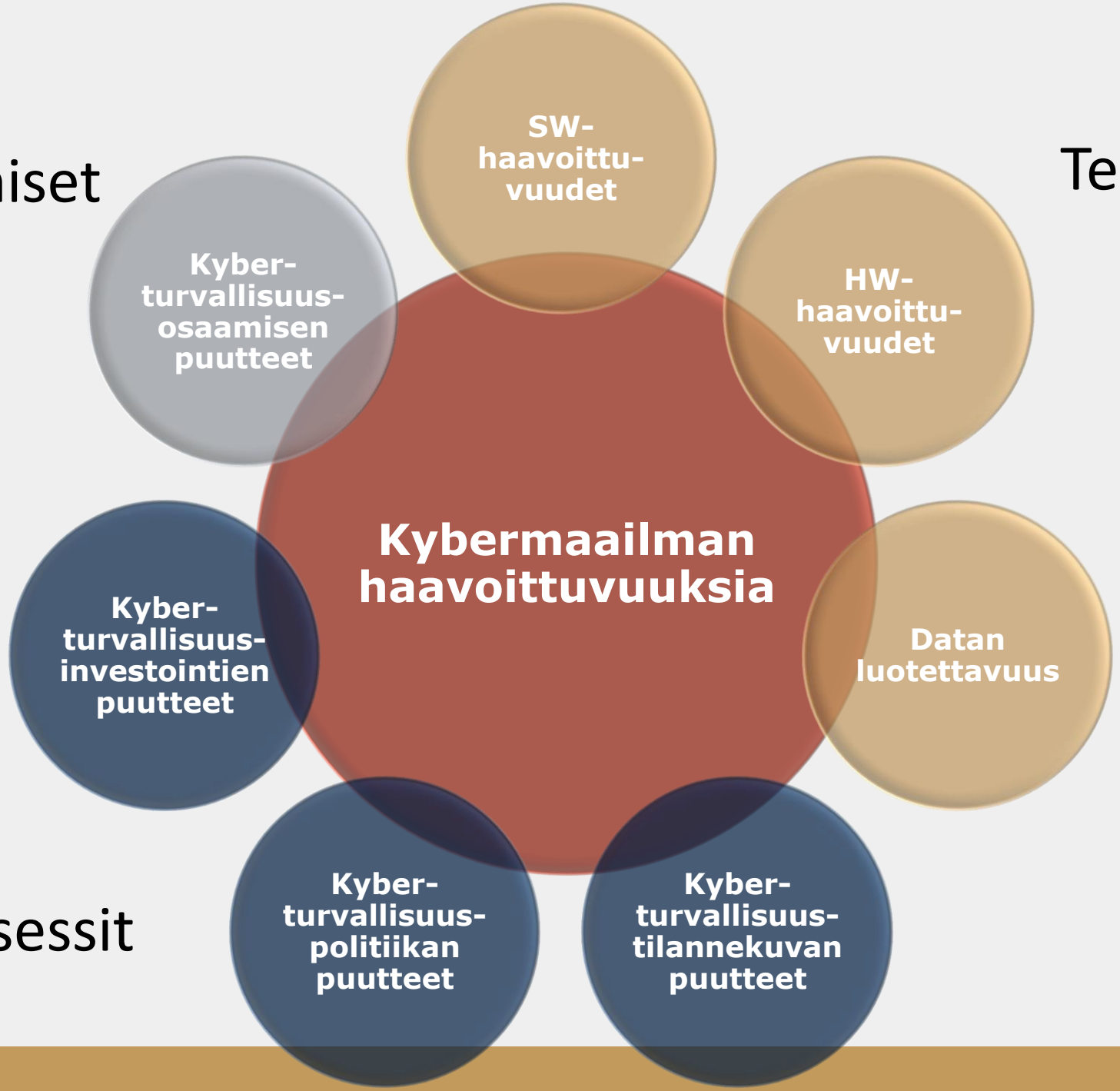
Esityksen sisältö

Uhka + haavoittuvuus = riski



Ihmiset

Teknologia

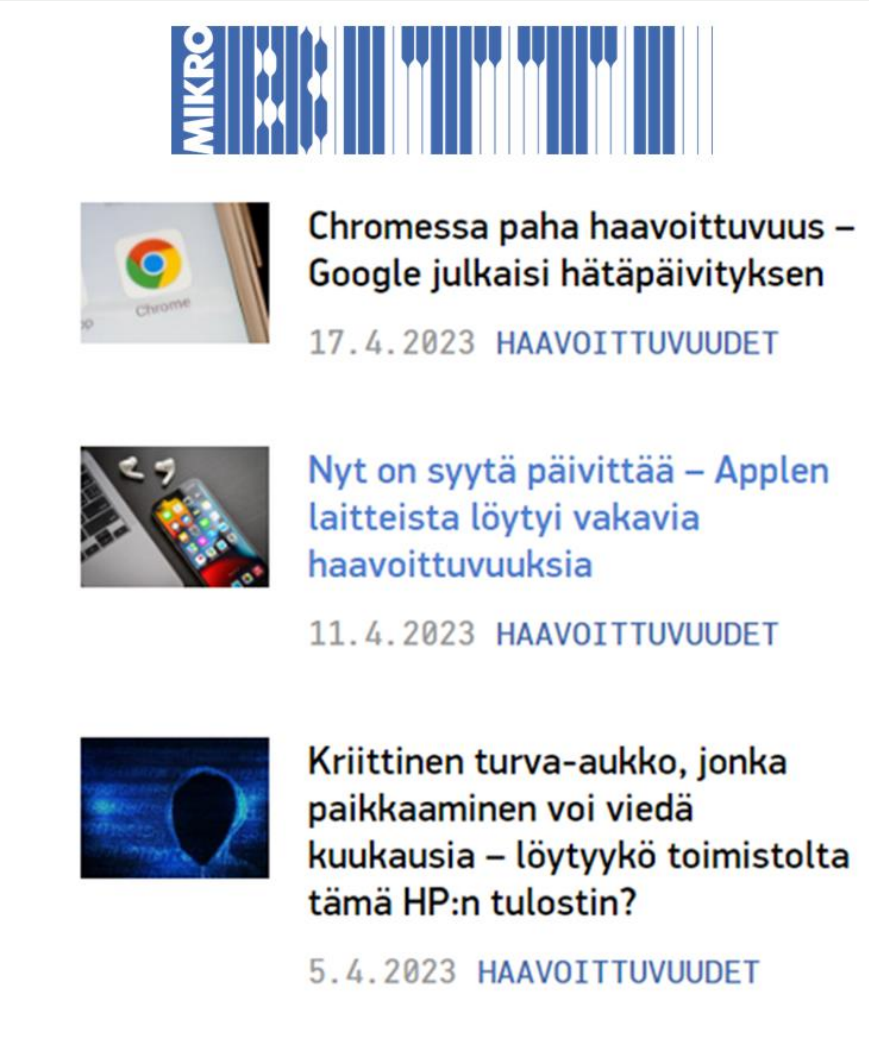


Prosessit

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

ILTA-SANOMAT TUOREIMMAT LUETUIMMAT SÄÄ Kirjaudu Hae Valikko

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

TIETOTURVA

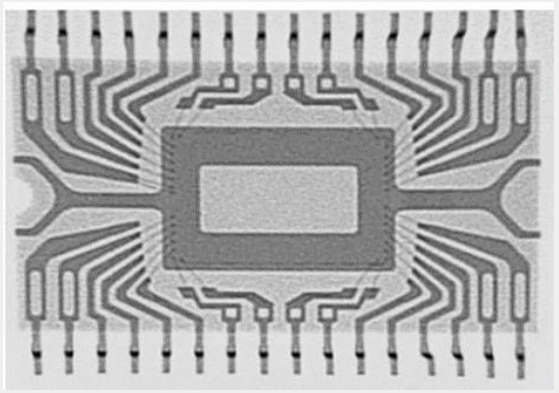
Haittaohjelma päätyi huippu-suosittuihin Android-sovelluksiin – ladattiin yli 100 miljoonaa kertaa

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

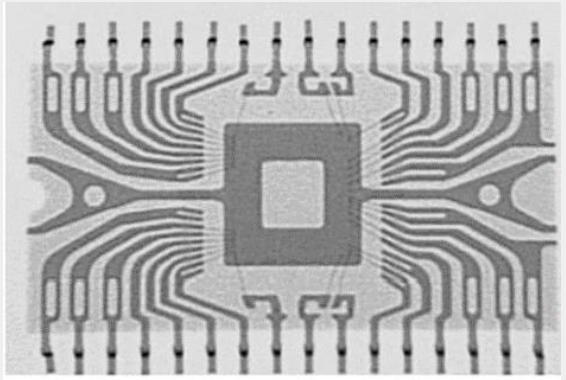
JAA KOMMENTOI

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
Component corruption

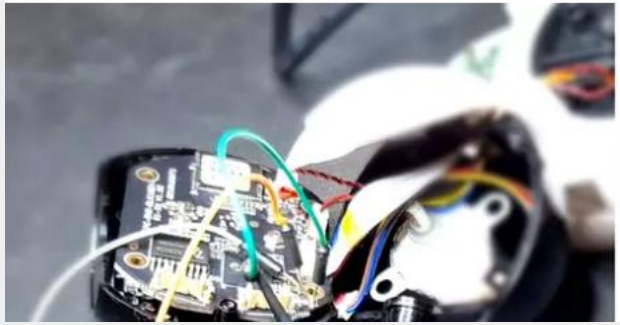


Röntgenkuvaus



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.



Sisäpiiriuhat

Pahantahtoinen sisäpiiriläinen

Käyttää mahdollisuutta päästä käsiksi sensitiiviseen tietoon ja tuottaa vahinkoa yritykselle.

Huolimaton sisäpiiriläinen

Altistaa organisaation toimimalla turvallisuusohjeiden vastaisesti

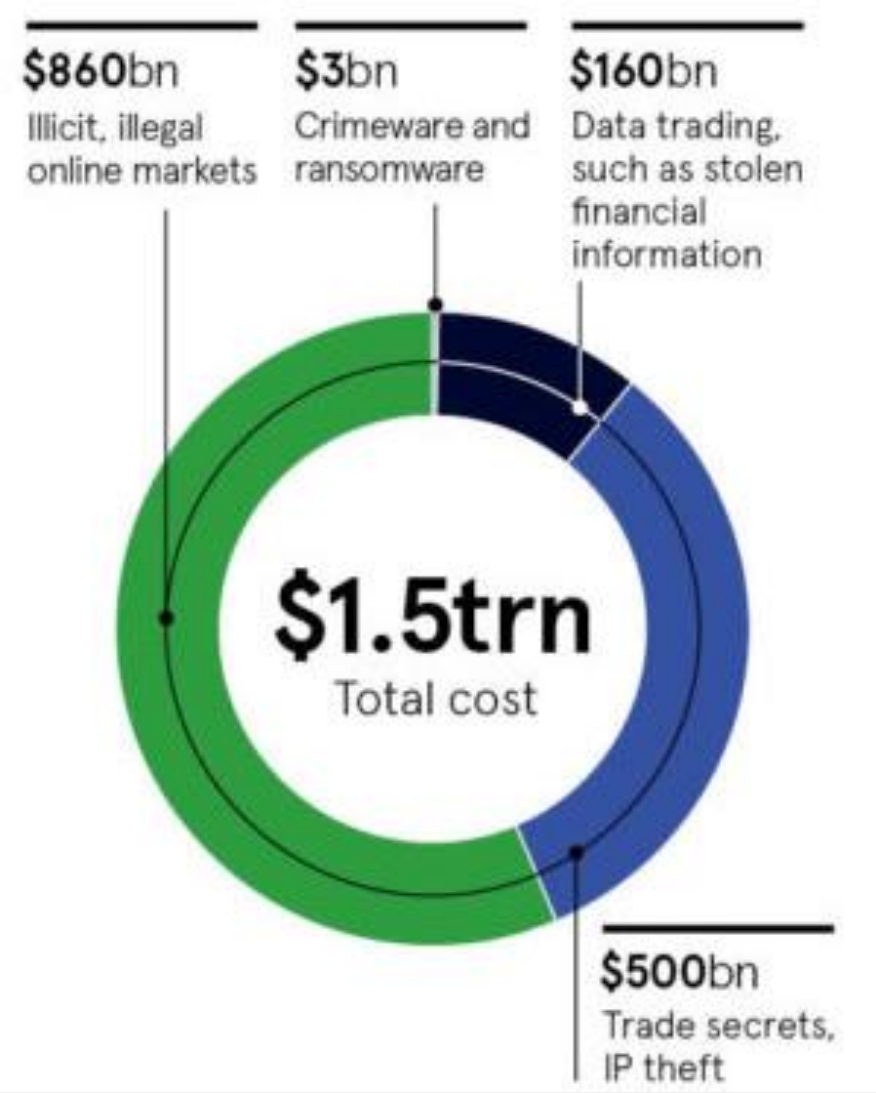
Hakkeroitu sisäpiiriläinen

Hänen käyttäjätilinsä on murrettu, vaikka hän on toiminut oikein.

Analyysien mukaan onnistuneissa kyberhyökkäyksissä 90 % mukana sisäpiiriläinen

Esityksen sisältö

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

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

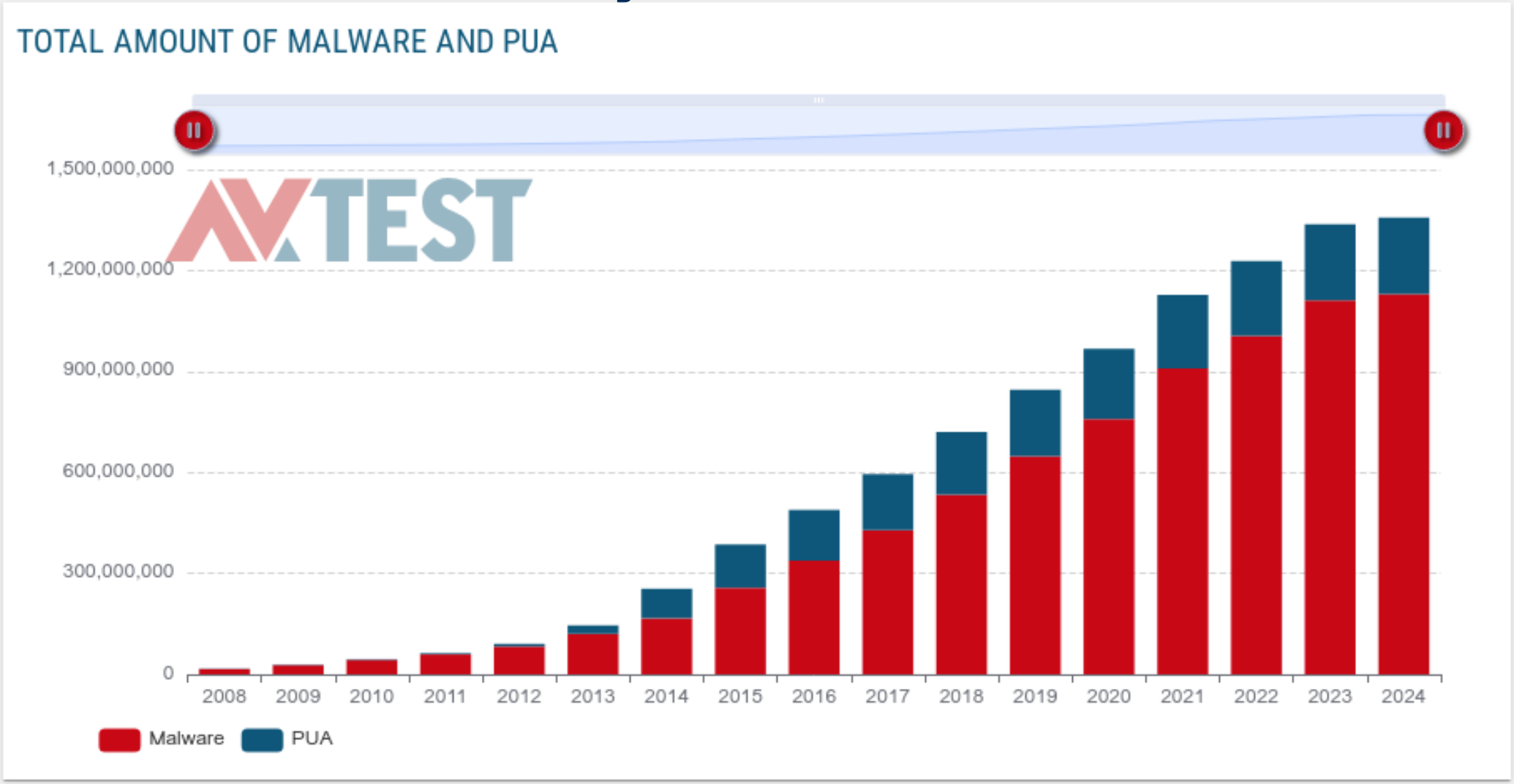
Sähköposti on edelleen verkkorikollisten suosikkikanava

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.

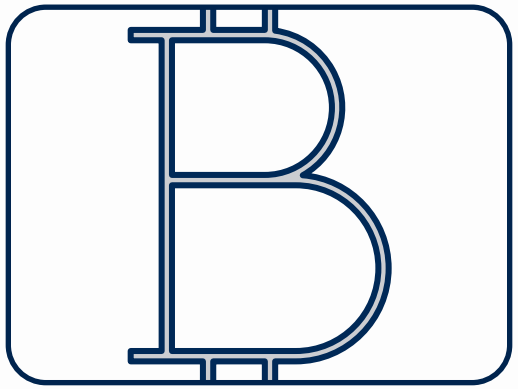
Haittaohjelmatuotanto



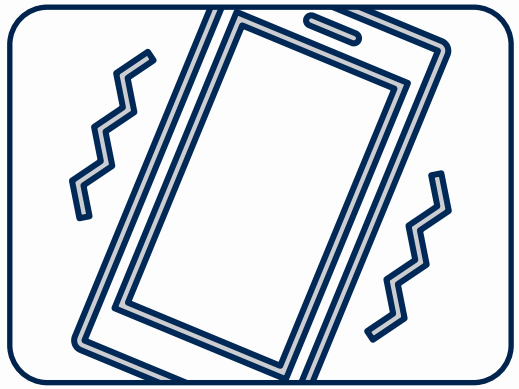
Source: AV-TEST, 20.5.2024

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.

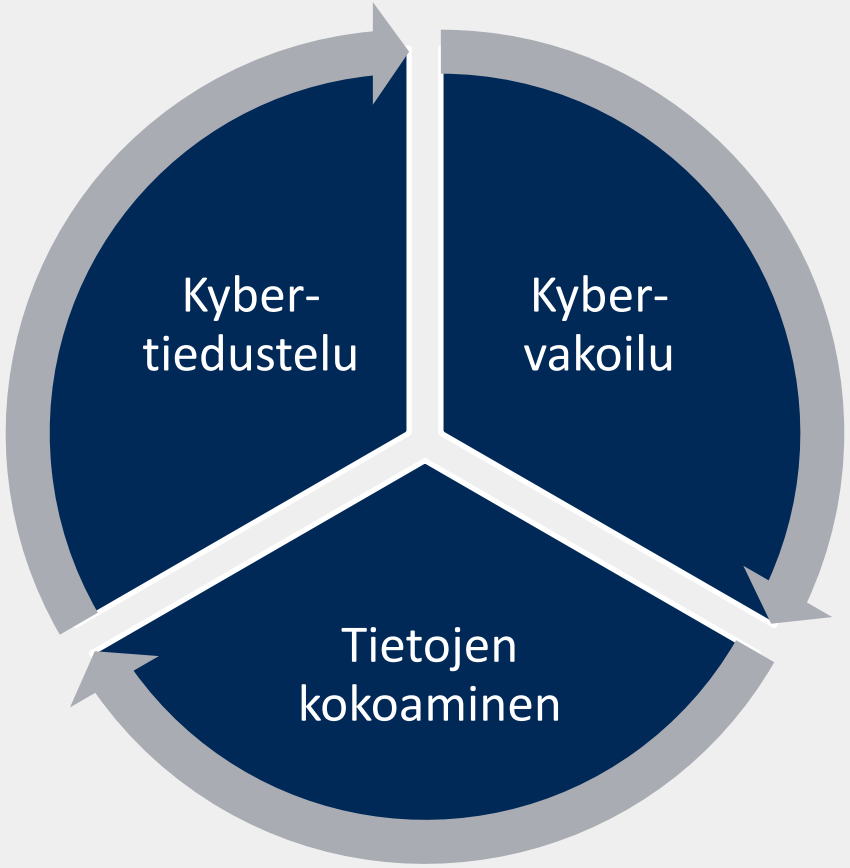
Palautus kesti 3 viikkoa
Tulon menetykset $42.1 miljoonaa
Kokonaistappio $67 miljoonaa

Esityksen sisältö

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)

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

Pegasus-vakoiluohjelma matkapuhelimessa

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

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

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 WhatsApp, Signal, ja Threema järjestelmissä. Turvallisuus ryhmäkeskusteluissa voi vaarantua.

SolarWinds kybervakoiluoperaatio

SolarWinds kybervakoiluoperaatio tuli julkisuuteen 13. joulukuuta 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:n 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.

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.

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

Esityksen sisältö

Kriittinen infrastruktuuri kyberhyökkäysten kohteena

Kyber-fyysisen toimintaympäristön rakenteet, ilmiöt ja tapahtumat ovat tiiviissä vuorovaikutuksessa muodostaen monimutkaisen ja keskinäisriippuvan kokonaisuuden.

Hyökkäyksillä kriittistä infrastruktuuria vastaan voidaan lamauttaa yhteiskunnan elintärkeitä toimintoja.

Kybersabotaasi

Stuxnet oli Windows-spesifinen tietokonemato, joka vakoili ja uudelleen ohjelmoi teollisuusjärjestelmiä. -> rikastusprosessin manipulointi.

Mato oli päässyt Iranin ydinlaitoksiin saastuneessa USB-muistitikussa.

Mitä tarvitaan onnistumiseen?

- Täydellinen tieto kohteen laitekonfiguraatiosta
- Tarvittavat sertifikaatit, jotta voidaan koodata ”luotettava” haittakoodi
- Kyky seurata vaikuttavuutta järjestelmän sisällä
- Kyky ohjata hyökkäystä tilanteen mukaan

Kriittinen infrastruktuuri kyberhyökkäysten kohteena

Chemical

Vuonna 2017 petrokemian laitos Saudi-Arabia

Dams

Vuonna 2016 Rye Brook Dam, New York. USA

Financial Services

Vuonna 2020 Banco Estado, Chile

Information Technology

Vuonna 2021 150 000 hyökkäystä viikossa

Commercial Facilities

Vuonna 2011 PNN Laboratorio Virginia USA

Defense Industrial Base

Vuonna 2007 kiinalaiset anastivat F-35 piirustukset

Food & Agriculture

Vuonna 2016 11 kyber-hyökkäystä, USA

Nuclear Reactors, Materials & Waste

Vuonna 2016 Gundremmingenin ydinvoimala, Saksa

Communications

Vuonna 2016 Dynin DNS-palvelu, USA + Eur

Emergency Services

Vuonna 2016 Dallasin poliisilaitos, USA

Government Facilities

Vuonna 2020 Suomen eduskunta

Transportation Systems

Vuonna 2015 LOT-lentoyhtiö, Puola

Critical Manufacturing

Vuonna 2015 terästehdas, Saksa

Energy

Vuonna 2017 EirGrid sähköyhtiö Irlanti

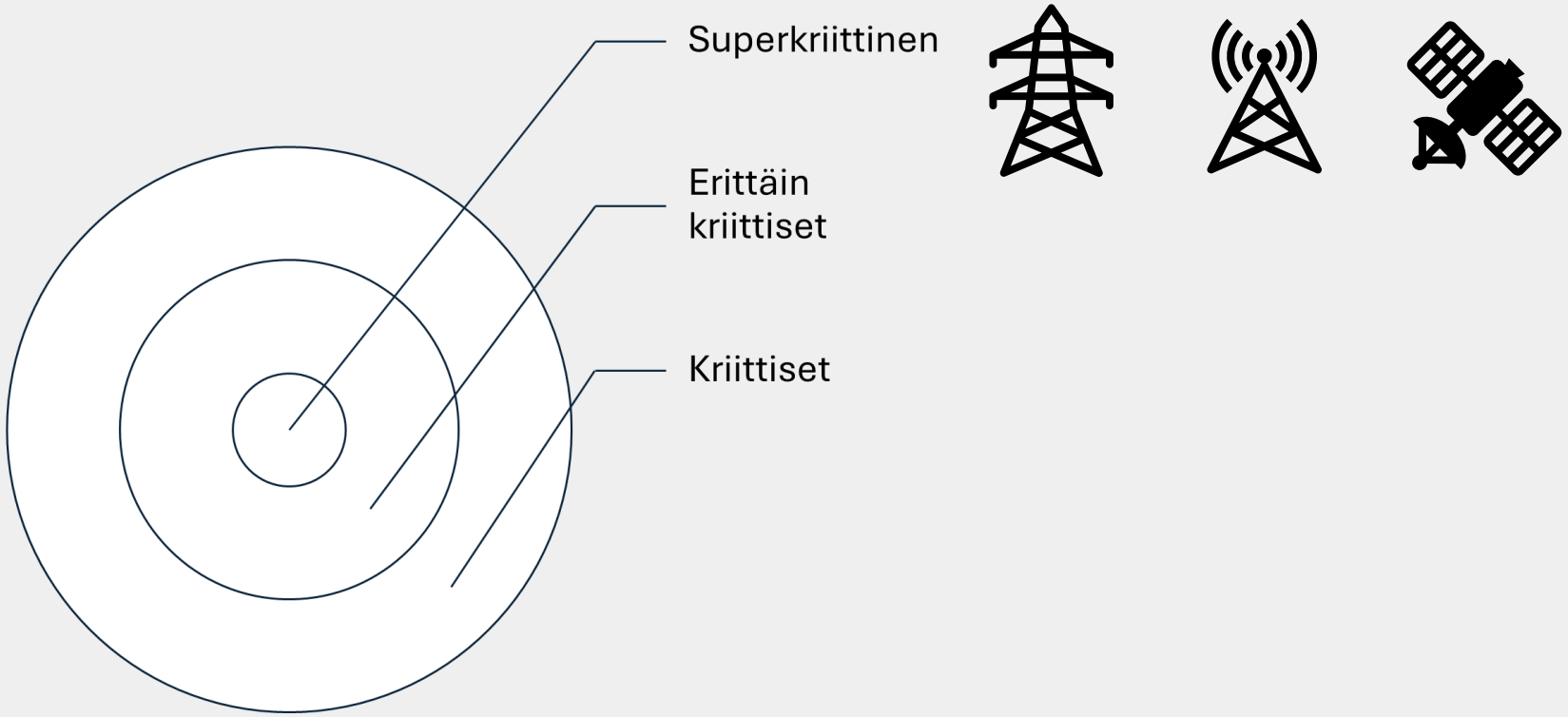
Healthcare & Public Health

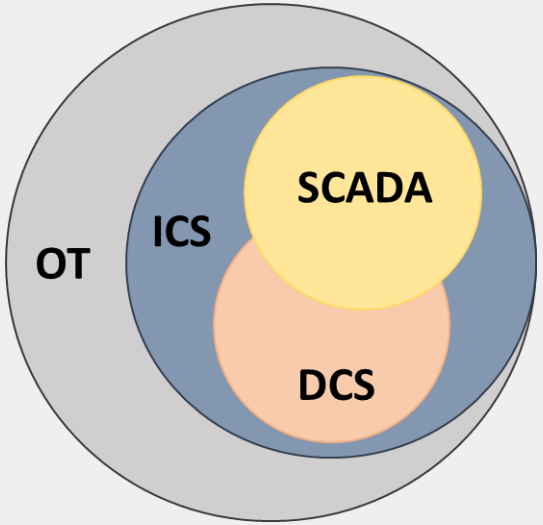
Vuonna 2017 Wannacy-hyökkäys laajasti

Water & Wastewater Systems

Vuonna 2020 Vesilaitos, Israel

Kriittinen vai superkriittinen?





Kriittisen kansallisen infrastruktuurin keskeiset osat ovat :

- Industrial Control System (ICS),
- Supervisory Control and Data Acquisition (SCADA) system,
- Distributed Control System (DCS), Operational Technology (OT).

Hyökkäys sähköverkkoon

Laaja sähköverkon lamautus kyberhyökkäyksellä joulukuussa 2015 ja 2016.

Ukrainalaisen sähköyhtiön 80 000 asiakkaalta onnistuttiin katkaisemaan sähkönsaanti haittaohjelmahyökkäyksellä kuudeksi tunniksi.

Tilannetta vaikeutettiin kohdistamalla energiayhtiön asiakaspalveluun häirintäsoittoja, jolloin asiakkaiden vikailmoitukset eivät päässeet läpi.

Datan tuhoava hyökkäys 25.2.2022

Tietoja tuhoava haittaohjelma levisi satoihin tietokoneisiin Ukrainassa. Samalla käynnistettiin verkkosivustoja kaatanut palvelunestohyökkäys.

Haittaohjelma tuhosi tietoja ja teki tietokoneesta toimimattoman.

Havaittiin myös Latviassa ja Liettuassa.

Kohteina on ollut sekä valtion että finanssialan alihankkijoita.

Hyökkäys Ukrainan satelliittilaajakaistaan, helmikuussa 2022

Hakkerit hyökkäsivät Ukrainan satelliittilaajakaistaan. Isku tapahtui samaan aikaan Venäjän hyökkäyksen kanssa.

Satelliitteihin kohdistunut sabotointi voi lamauttaa Ukrainan taistelukyvyn, koska Viasat on toimittanut internetyhteyden Ukrainan asevoimien ja poliisin yksiköille.

Paikannussatelliittijärjestelmien häirintä 17.3.2022

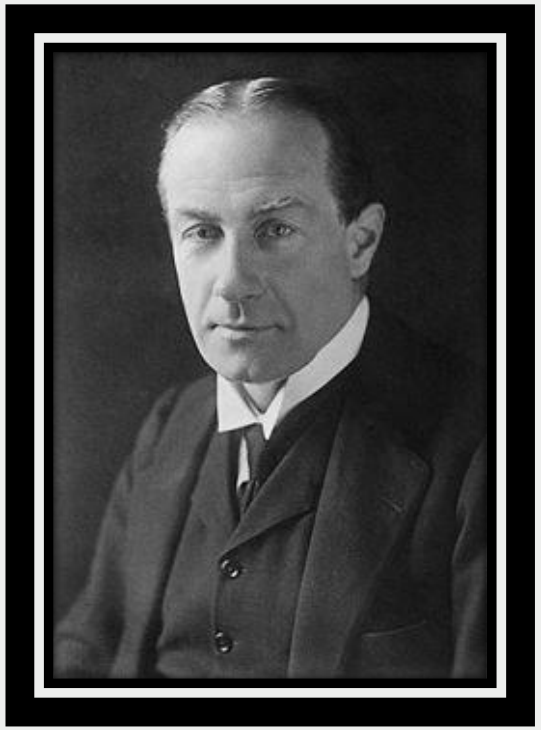
Paikannussatelliittijärjestelmiä on häiritty Venäjän hyökkäyksen alkamisen jälkeen eri alueilla.

Häirintää on ilmennyt itäisessä Suomessa, Kaliningradin alueen ympäristössä, Mustalla merellä, sekä itäisen Välimeren alueella Kyprosta, Turkkia, Syyriaa, Israelia ja Pohjois-Irakia myöten.

Häirinnän vuoksi lentokoneet ovat joutuneet paikoin vaihtamaan reittiä kesken lennon tai jopa vaihtamaan määränpäätä, sillä häirintä on estänyt turvallisen laskeutumisen alkuperäiseen kohteeseen.

Esityksen sisältö

”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***."

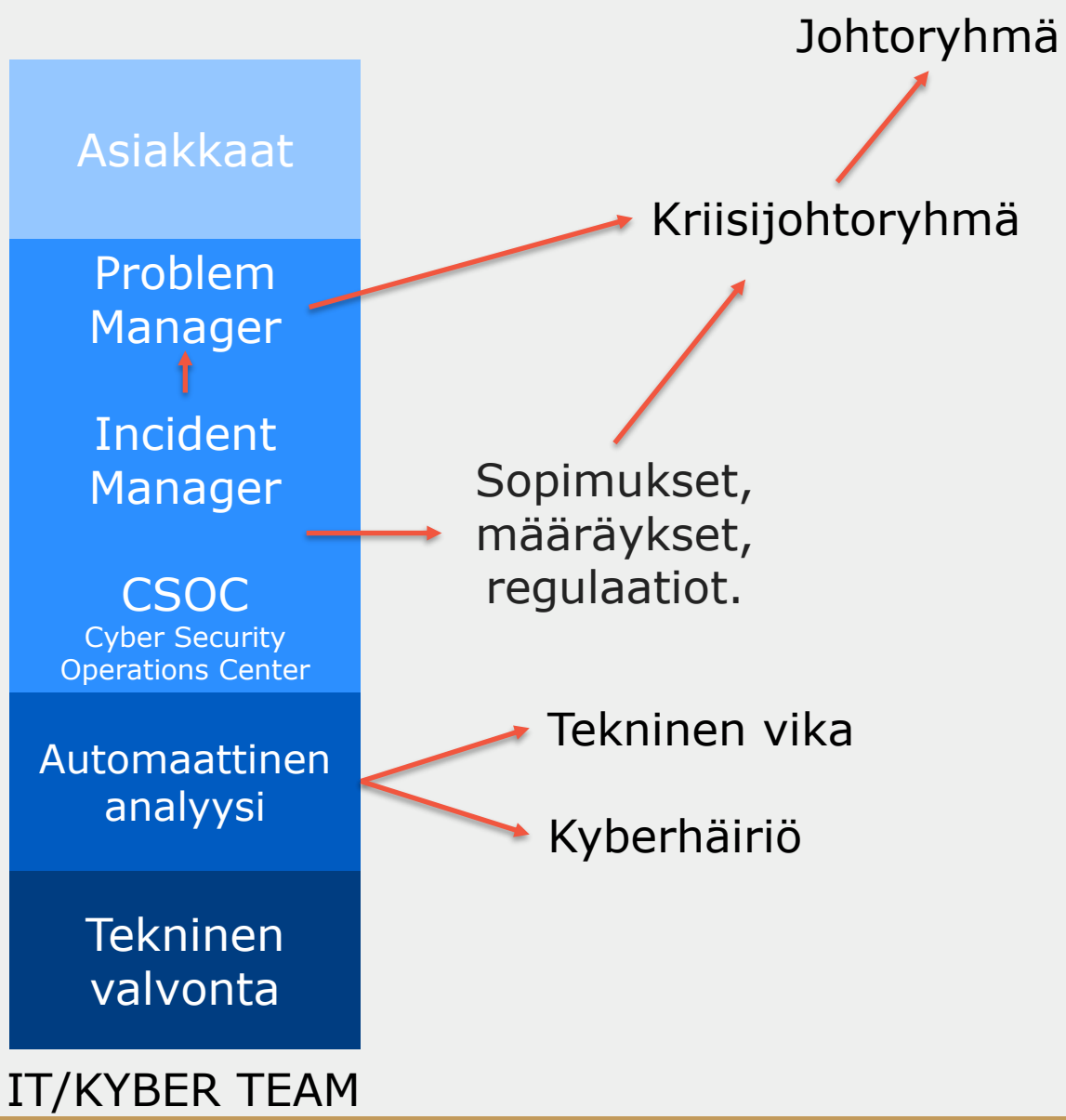
Speech in House of Commons of the Parliament of Great Britain in November 1932.

→ ”Kyberhyökkäys pääsee aina läpi”

Kyberturvallisuuden johtaminen - tehtävät ja vastuut

ASSET OWNER VASTAA		TIETOTURVATIIMI TUKEE	YRITYSJOHTO SITOUTTAA
Pääsyoikeuksien valvonta	**Tuotanto-omaisuuden hallinta**	**Suunnittelu ja kehitys**	**Henkilöstön johtaminen**
Tunnusten ja salasanojen oikea käyttö	Tuotantolaitoksen kokonaisuus	Kyberturvan kehitys-ryhmän perustaminen	Roolien ja vastuiden määrittely
Etäyhteyksien valvonta	Valvomotilat ja järjestelmät	Vuosisuunnitelman laadinta	Tehtävien määrittely, riittävän resursoinnin takaaminen
Fyysisen pääsyn valvonta	Sähköverkon järjestelmät	Kyberturvan minimivaatimukset	Koulutusmahdollisuudet
Tutkinnan käynnistäminen	Kaukokäyttöverkon järjestelmät	Ratkaisujen evaluointi	Sopimusmallit ja sitoumukset
Loukkausten kommunikointi	Tietoliikennejärjestelmät ja verkot	Pilotoinnit ja kehitysprojektit	Osaamisen johtaminen, kehittäminen ja jakaminen
	Järjestelmien hallinta	**Kyberturvan jalkautus**	**Kumppanuuksien hallinta**
	Asennukset, muutokset ja poistot	Ohjeiden laadinta ja koulutus	Kumppanien arviointi ja valinta
	Päivitykset, korjaukset, kovennus	Mallien laadinta ja koulutus	Sopimukset ja kumppanien velvoitteet
	Varmuuskopiointi ja palautus	Oikeiden toimintatapojen kuvaus	Kumppanien vastuiden määrittely
	Inventaario, kirjaukset ja dokumentointi	Raportoinnin kuvaus ja harjoittelu	Yrityksen ohjeiden ymmärrys
	Arkkiteht. ja verkkosegmentointi	Jalkautus ja seuranta – yleensä	Kumppanien toiminnan seuranta

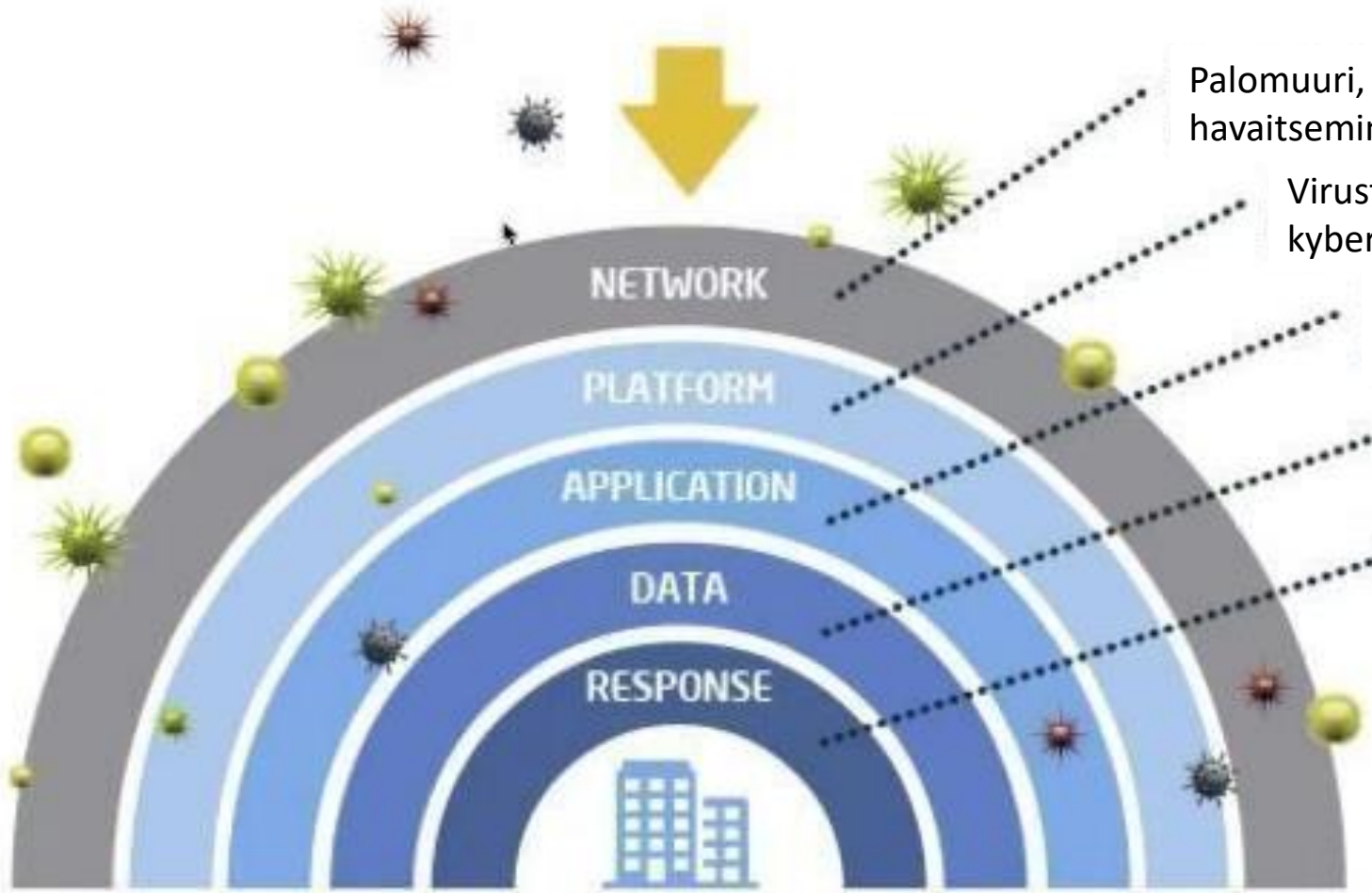
Esimerkki tilannekuvasta ja johtamisesta



- Reaaliaikainen tilannekuva- ja ymmärrys
- Häiriötilanteiden johtaminen
- Jatkuvuuden hallinta

Perusta:
- Selkeä organisaation toimintaprosessi ja pelikirja häiriötilanteissa

Kyberturvallisuusteknologia: Kerrossuojaus



Palomuuri, tunkeutumisen havaitseminen ja esto (IDS/IPS

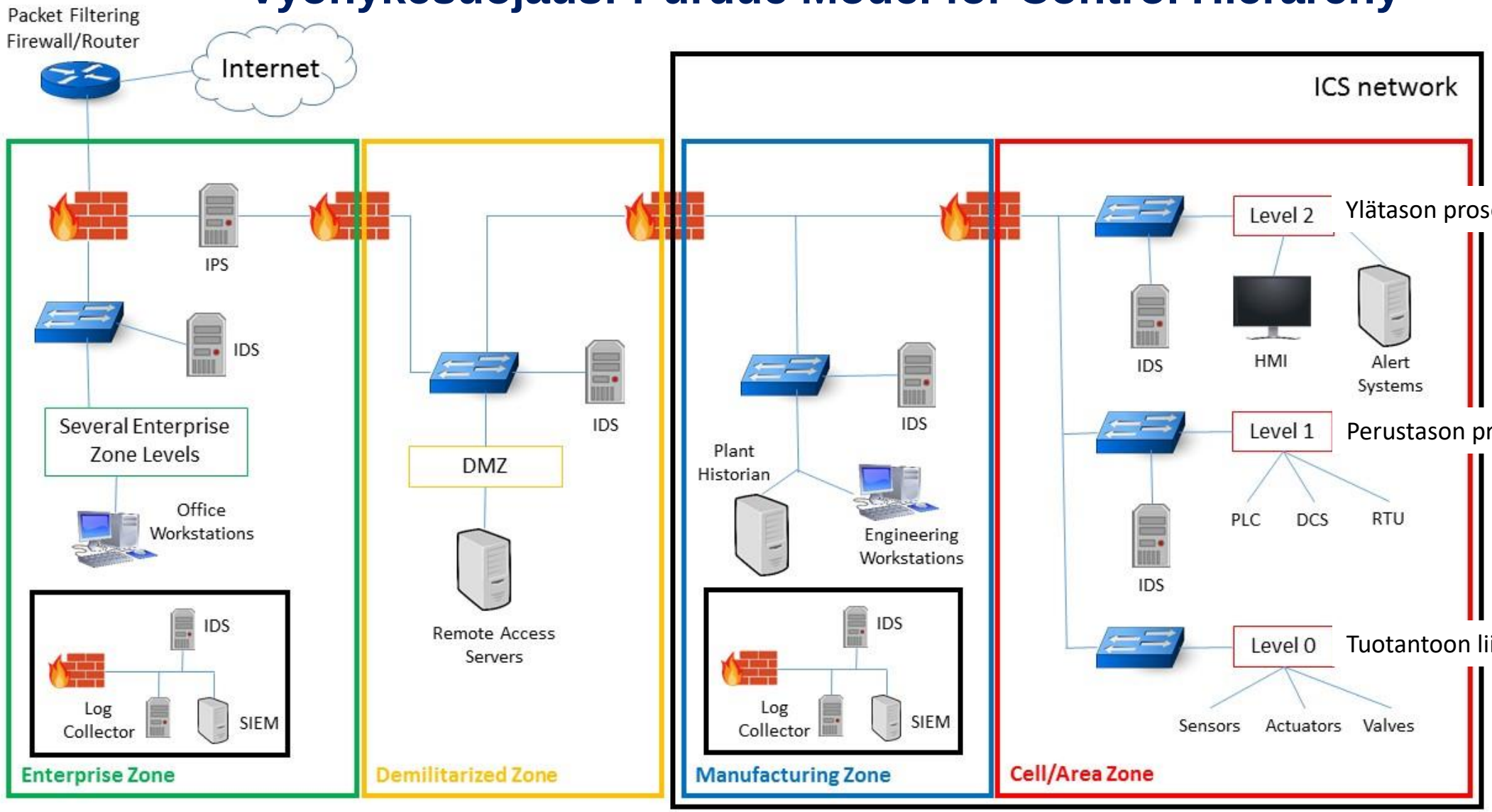
Virustorjunta, paikkaus/korjaus, kyberturvallisuusalustaratkaisut

Turvallinen koodaus, turvallisuusratkaisut,

Tiedosto ja datasalaus, pääsyoikeudet

Monitorointi (SIEM), anomalioiden havaitseminen, korjaustoimenpiteet

Vyöhykesuojaus: Purdue Model for Control Hierarchy



Ylätason prosessivalvonta

Perustason prosessivalvonta

Tuotantoon liittyvät sensorit

Internetin kautta tarjottavat palvelut

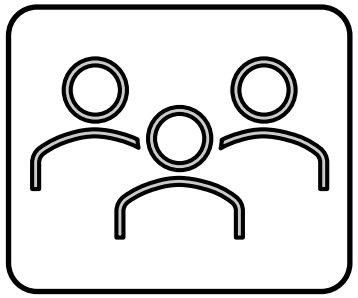
Kaikki tietoliikenne ohjataan valvotun DMZ:n kautta

Tuotantoympäristö

Turvallisuuden valvontaympäristö

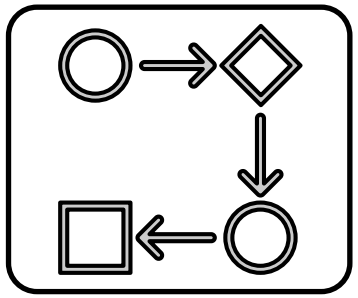
Source: Obregon, L. (2015) Secure Architecture for Industrial Control Systems. SANS Institute InfoSec Reading Room.

PPT-vahvistaminen



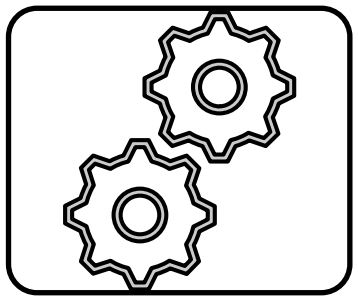
Ihmiset

- Osaamisen johtaminen ja kehittäminen
- Turvallisuuskulttuurin ja johtamisen kehittäminen
- Osaamisen sertifiointi



Prosessit

- Virtaviivainen kyberturvallisuuden johtamisprosessi
- Kaikkien prosessien hallinta (normaali – epänormaali)
- Häiriötilanteiden hallinta – jatkuvuuden hallinta



Teknologia

- Kyberturvallisuusarkkitehtuuri
- ICT-ympäristön tilannetietoisuus
- Sertifioidut laitteet

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

Kiitos

www.jyu.fi/it