Aalto-yliopisto
Sähkötekniikan korkeakoulu

Kyberuhat tavoittavat automaation

Mikko Särelä, Seppo Tiilikainen,Timo Kiravuo
Aalto-yliopisto
Sähkötekniikan korkeakoulu
Tietoliikenne- ja tietoverkkotekniikan laitos
timo.kiravuo@aalto.fi

Mitä "kyber" tarkoittaa

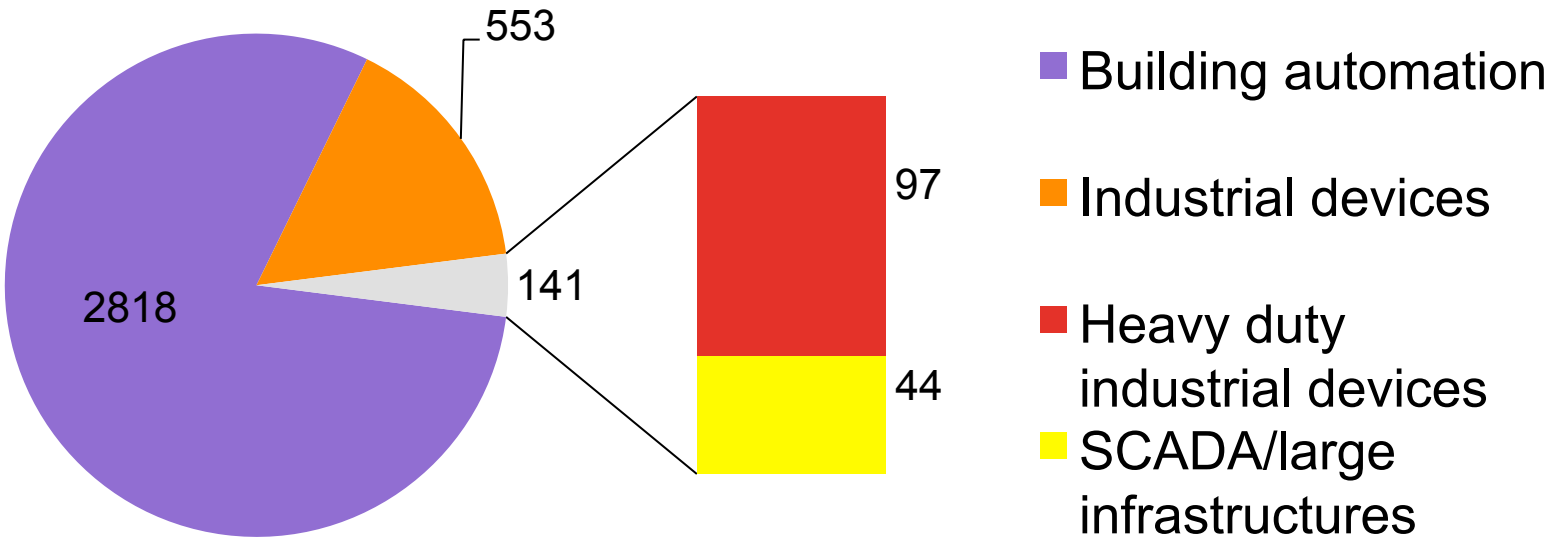
- Historia:
  - Kybereo (kreik.): ohjata, hallita
  - κυβερνήτης (kybernētēs): ohjaaja
  - Kybernetiikka: säätötekniikka
- Nykyään:
  - Kyber: tieto- ja tietokonejärjestelmiin liittyvä (Kyberturvallisuusstrategia 2013)
  - Kyber: digitaalisiin järjestelmiin liittyvä (prof. Jukka Manner 2012)
    - Kattaa myös automaation ja sulautetut järjestelmät

Automaatio ja tietoturva

- Tietoturva: suojaa **tietoa** väärinkäytöksiltä
  - Yleisratkaisu: estä pääsy lukemaan tietoa,
  - Jos lukeminen sallittua, estä tiedon muuttaminen
- Automaatio toteuttaa **prosessia**
  - Yleisratkaisu: prosessin on toimittava ja oltava ohjattavissa kaikissa tilanteissa
  - Turvallisuus suojaa ihmisiä ja laitteita vahingoilta
- Automaatiojärjestelmissä heikko sisäinen suojaus
- Automaation tietotekninen turvallisuus perustuu järjestelmien saavuttamattomuuteen
  - Erillään Internetistä
  - Palomuurien takana
  - Vahva pääsynhallinta

Mitä Suomen Internetistä löytyy?

- 3700 laitetta
- 60% laitteista on olemassa tunnettu haavoittuvuus
- Kevät 2013



Suomen Internet

- Tärkeitä teollisuuden järjestelmiä (ICS, SCADA): 141 laitetta
- 553 muuta teollisuusautomaatiolaitetta, useimmat etähallinnan yhteyskäytäviä
- Hieman yli 2800 rakennusautomaatiojärjestelmää, suurin osa web-käyttöliittymiä. (mm. asuintaloja, kauppoja, pankin toimisto, jäähalli, vankila)
- Jälkitarkastuksessa löytyi näistä 1968 laitetta online-tilassa (tavoitettavissa)

Miten laitteita etsitään?

- Internetin osoitteisiin voidaan lähettää tietoliikennepaketteja ja katsoa mitä saadaan vastaukseksi
  - Porttiskannaus
- Jos osoitteessa on kone, eri protokollaosoitteiden vastauksista voidaan tunnistaa käyttöjärjestelmä ja versio
  - Fingerprinting
- Shodan on julkinen hakukone, jota voidaan käyttää tähän

Shodan

- http://www.shodanhq.com/
- Käy Internetin osoitteita läpi kuten muut hakukoneet
- Tallettaa tiedon eri tietoliikenneporteista saatavista vastauksista
  - Protokolla
  - Ohjelmistoversio yms. tietoa
- Mahdollistaa kohteen tunnistamisen sen palveluiden perusteella
- Shodan ei ole kattava, skannaa satunnaisesti vain osan verkosta

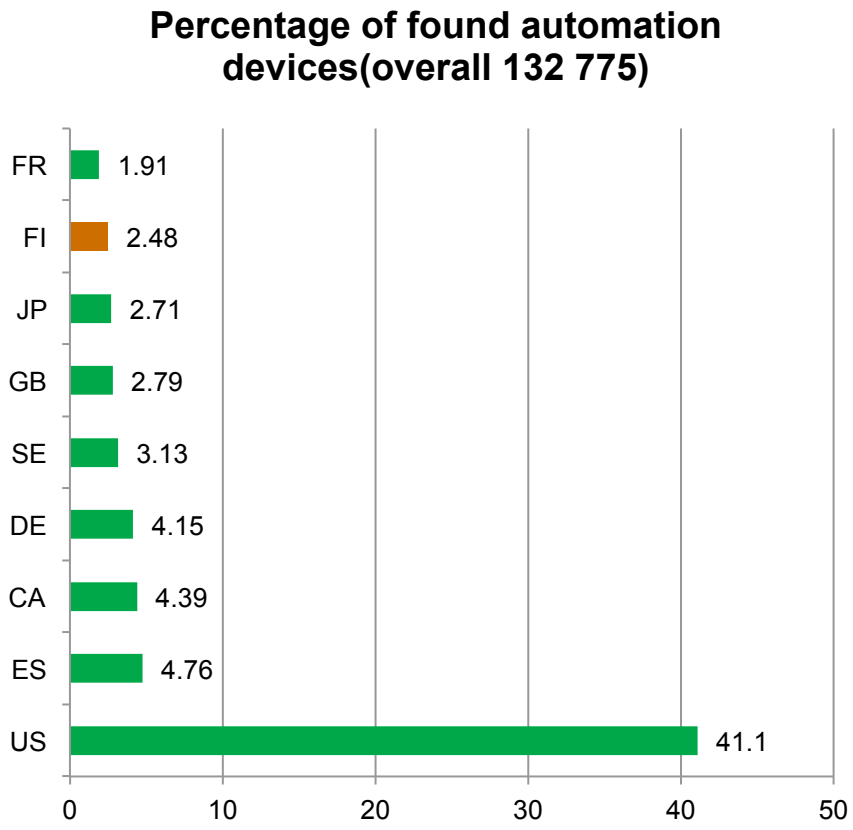
Shodanin käyttö

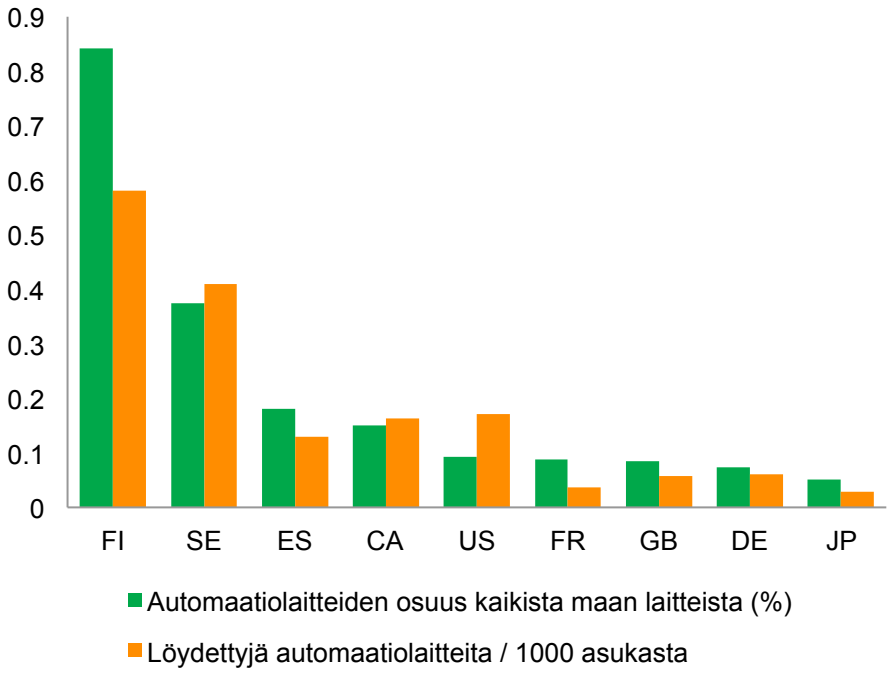
- Hakusanalla "EnergyICT" löytyy RTU -webliittymiä
  - Etenkin Elster EnergyICTn tuotteita
  - http://energyict.com/

Shodanin käyttö

- Haku "SpiderControl 200 OK" löytää SpiderControlin käyttöliittymiä
  - http://spidercontrol.net/
- "200 OK" viitaa siihen, että palvelin suostuu kommunikoimaan

Suomi hyvin edustettuna



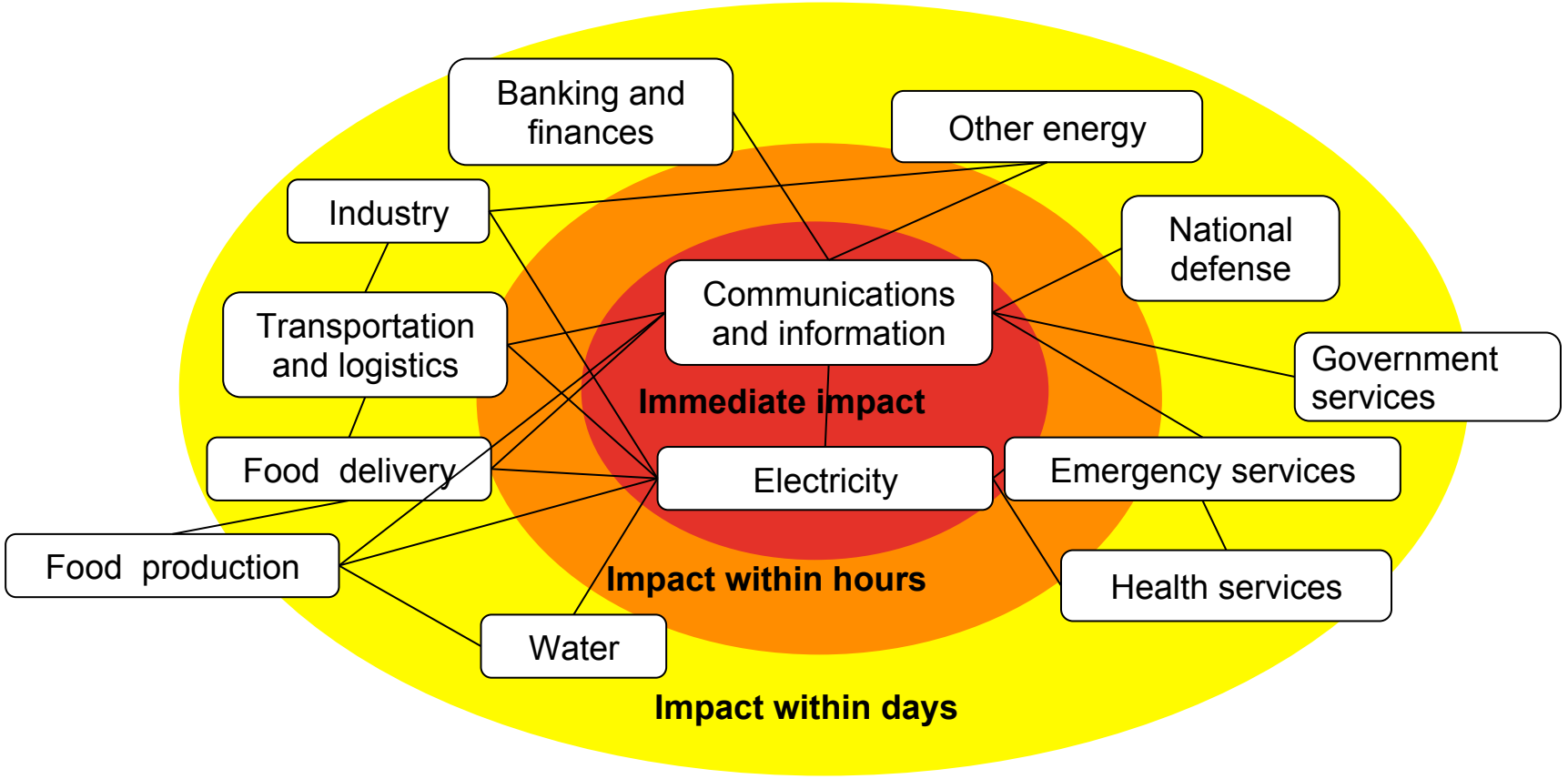


Seppo Tiilikainen, Aalto

Kansallinen hakukone KATSE

- Aallossa toteutetaan Shodania vastaava toiminnallisuus Suomen verkon kartoittamiseksi
- Haluamme että tieto pysyy Suomen sisällä
- Tukee viranomaistoimintaa
- Palaute järjestelmien omistajille
- Rajoituksena rikoslain 38. luku ja tietomurto
  - Saamme ottaa yhteyttä verkossa olevaan koneeseen
  - Emme saa kokeilla tunnettuja oletussalasanoja tai haavoittuvuuksia
- Pyrimme vastaamaan kansallisen kyberturvallisuuden yhteen ydinkysymykseen:
  "Miten haavoittuva Suomi on?"

Kriittisen infrastruktuuri riippuvuudet



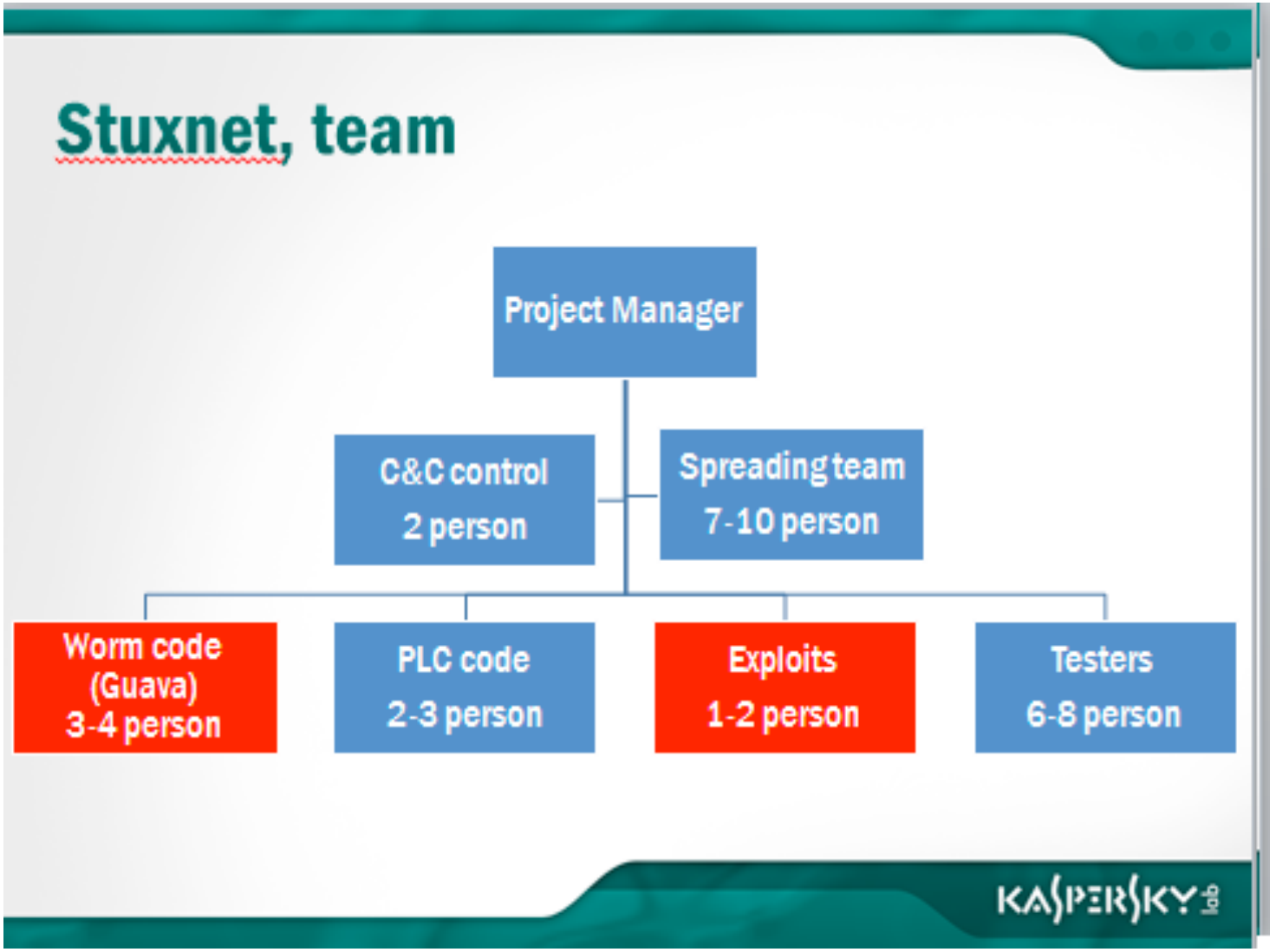
- Kuinka nopeasti yhteiskunta hajoaa

Kyberhyökkäys: Stuxnet

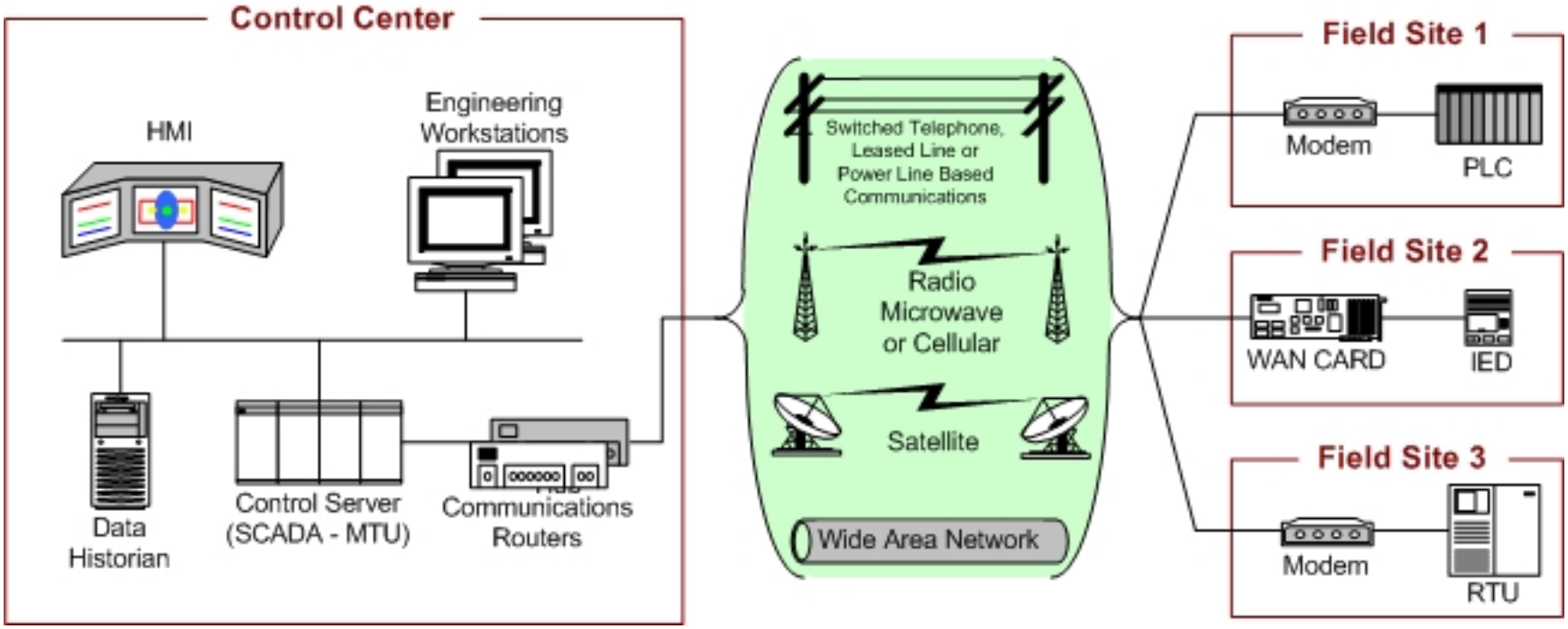
- Täsmähyökkäysohjelmisto, räätälöity itsekopioiva mato
  - Kohteeseen USB-tikulla
- Kohde: Iranin Natanzin uraaninrikastuslaitos
- Tavoite: hidastaa Iranin ydinohjelmaa
  - Tunkeutui SCADA-ohjausjärjestelmään, uudelleenohjelmoi PLC-kontrollerit
- Suorittaja: USA Israelin avustamana
- Vaikutus: Iranin ydinohjelman hidastaminen usealla vuodella
- Valtiollinen operaatio, jolla selkeä strateginen tavoite

Arvio Stuxnetin projektiryhmästä

- 22-30 henkilöä
- Lähde: Kaspersky

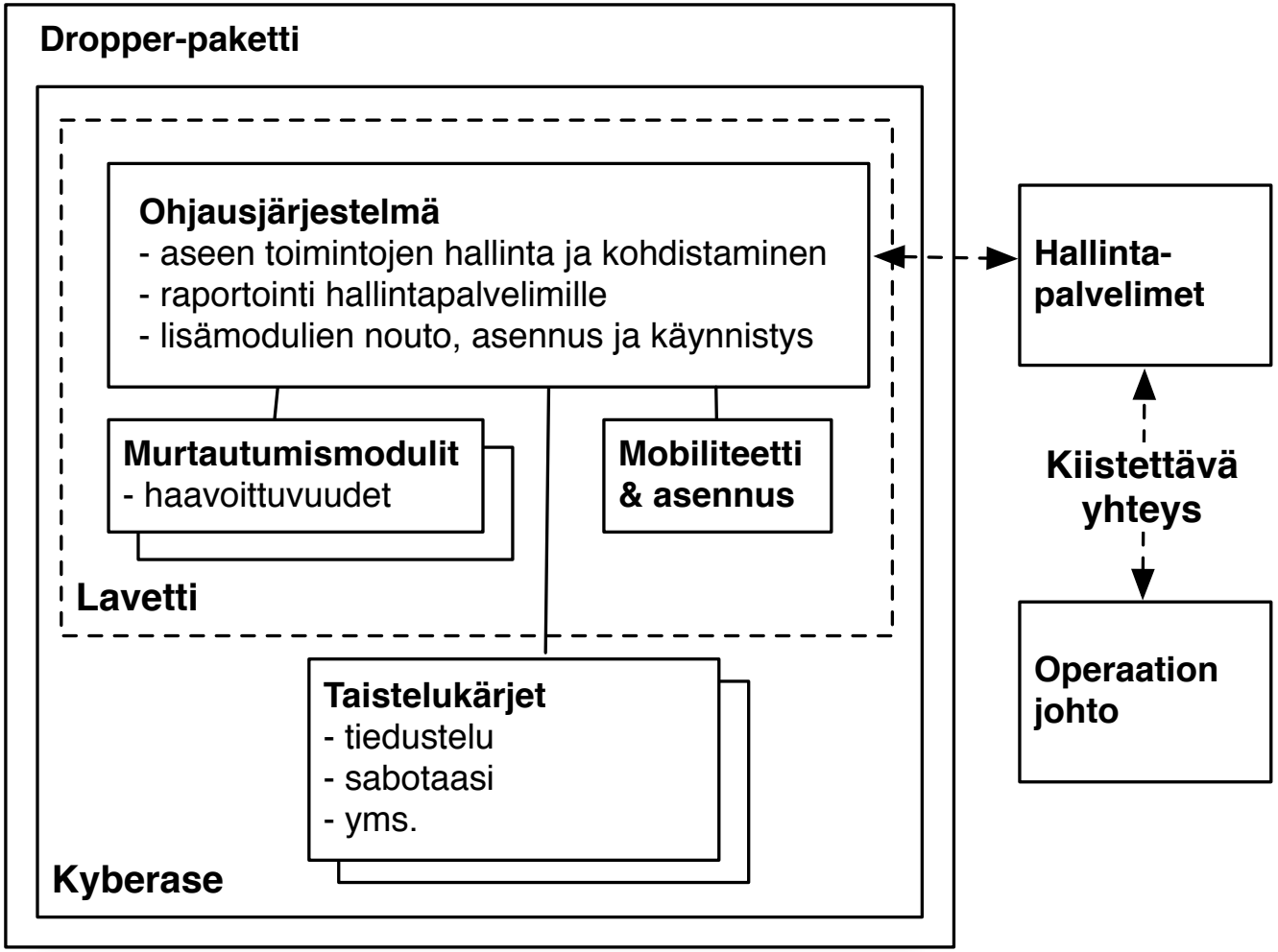


Teollisuusautomaatio kohteena

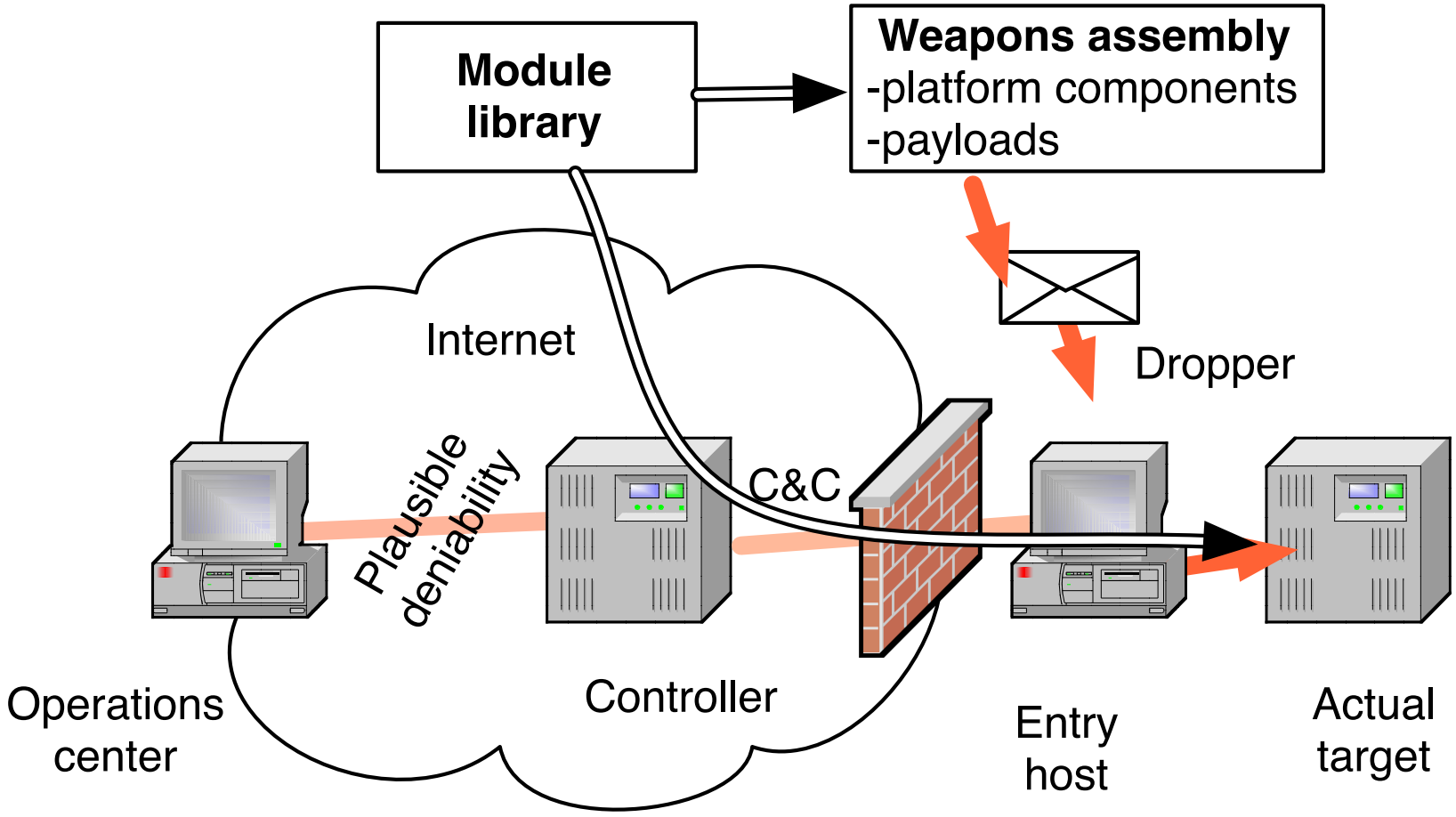


[NIST SP 800-82]

Uhka: Modulaarinen hyökkäysohjelma (kyberase)



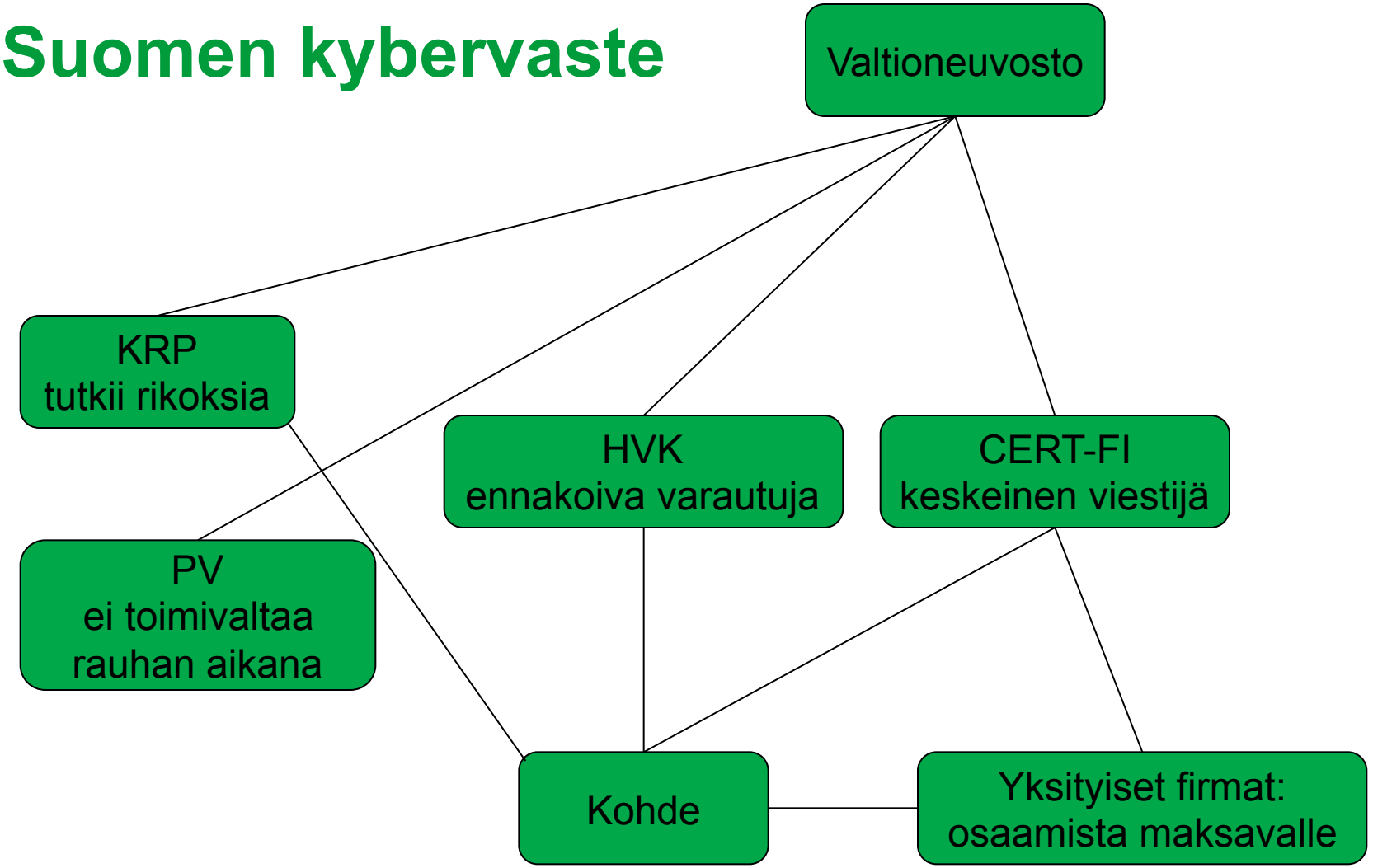
Kyberoperaatiot



Kyberuhan lähteet

Uhkaaja	Motivaatio	Tavoite
Valtio	taloudellinen, vaikutusvalta	vastustajan toimien estäminen, informaation kerääminen
Rikollisuus	taloudellinen	tiedon myynti eteenpäin, kiristys, pääsy varsinaiseen kohteeseen
Yritykset	taloudellinen	kilpailijan häiritseminen, informaation kerääminen
Terroristit	yhteiskuntajärjestyksen muuttaminen	yleinen epäjärjestys, vastustajien vahingoittaminen
Muut poliittisesti aktiiviset tahot (hacktivismi)	valta	vastustajan saaminen huonoon valoon, informaatio
Utelias ihminen	kokeilunhalu	painella nappuloita ja katsoa mitä tapahtuu
Työntekijä	oma etu, kosto	taloudellista hyötyä, vahinkoa organisaatiolle

Suomen kybervaste



Anna Leppänen, TY & PolAMK ja Timo Kiravuo, Aalto

Suomen kyberpuolustus ja -turvallisuus

- Kyberturvallisuusstrategia 2013 ja aiempi julkishallinnon linjaus jakaa vastuut hallinnonaloittain
- Viestintäviraston CERT-FI -toiminto kerää ja jakaa tietoa ja toimii aktiivisesti tietoturvaongelmien ratkaisemisessa
- Huoltovarmuuskeskus ohjaa oman toimialansa yrityksiä kehittämään turvallisuuttaan ja rahoittaa osan CERT-FI:n toiminnasta
- N. 80% kriittisestä infrastruktuurista on yksityisen sektorin hallinnassa
- Poliisi selvittää rikoksia ja priorisoi rikoksen vakavuuden mukaan
- Puolustusvoimat suojaa omat järjestelmänsä ja kehittää sotilaallisia kyberkykyjä, ei näe itseään toimijana rauhan aikana
- Viranomaisilla on omaa analyysikapasitettia, mutta merkittävä osa hyökkäyksien teknisestä analyysikyvystä on yksityisellä sektorilla
- Käytännössä em. tahot tekevät aktiivista yhteistyötä, paljolti ad-hoc-pohjalta
- Kyberturvallisuusstrategiassa määriteltyä organisaatiota ei ole vielä testattu tositoimissa

Entä suojaus?

- Normaalit tietoturvatekniikat ja -käytännöt
  - Ei "hopealuotia"
- Uhkien teknologia ei ole olennaisesti muuttunut
- Uhkien intensiteetti on noussut
  - Valtio toimijana
  - Järjestäytynyt rikollisuus tarjoaa kaupallisena palveluna
- Kohteena muukin kuin tieto
  - Jatkossa yhä useampi laite on verkossa kiinni
  - Rakennus- ja teollisuusautomaatio, "Internet of things", ajoneuvot...

Yhteenveto

- Suomi on haavoittuva
  - Osaava hyökkääjä voi aiheuttaa merkittävää vahinkoa yhteiskunnan kriittiselle infrastruktuurille
  - Automaatiojärjestelmät osa kokonaishaavoittuvuutta
- Suomen turvallisuustilanne on hyvä
  - Suomi ei ole aktiivisen uhan kohteena
- Nyt on hyvä ajankohta nostaa turvallisuustasoa
  - Normaalien kehitystoimenpiteiden myötä
  - Kohtuullisin kustannuksin