JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

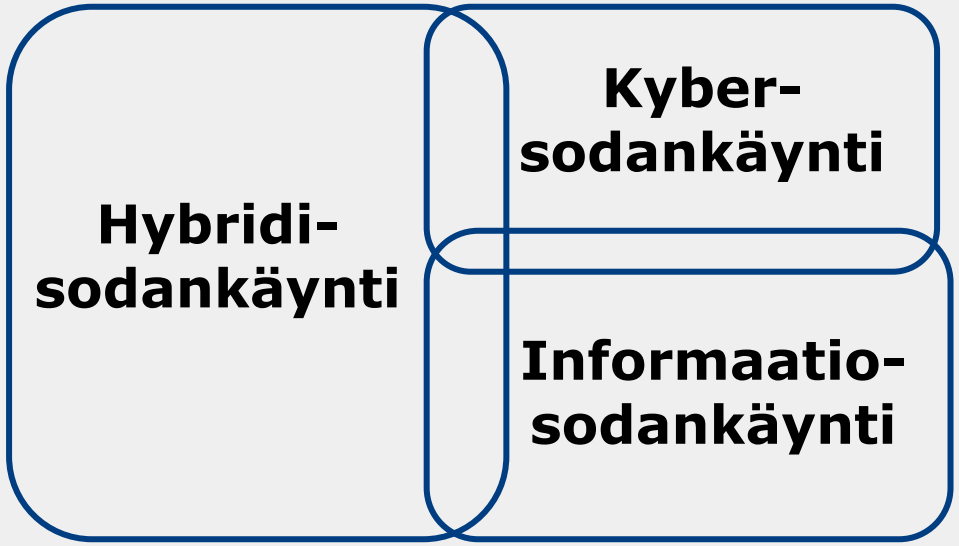
Ajankohtaisselonteko turvallisuusympäristön muutoksesta, VNS 1/2022 vp

Professori, ST Martti Lehto

29.4.2022

Sodankäynnin paradigman muutos

Hybridisodankäynnissä yhdistellään sotilaallisia, taloudellisia, poliittisia ja muita ei-kineettisiä toimia poliittisten, sotilaallisten ja taloudellisten päämäärien saavuttamiseksi.



Kybersodankäynnin operaatioin vaikutetaan digitaaliseen kriittiseen infrastruktuuriin = kybertilan hallinta.
War in bits and bytes.

Informaatiosodankäynnin operaatioin vaikutetaan poliittiseen ja sotilaalliseen päätöksentekoon sekä kansalaisten mielipiteisiin = informaatioylivoima.
War on Minds

Strategisella, operatiivisella, taktisella tasolla

Digitaalisen maailman murros

Venäjän käynnistämä sota vaarantaa koko Euroopan turvallisuuden ja vakauden.



Kyberoperaatioilla voidaan lamauttaa yhteiskunnan kriittistä infrastruktuuria ja elintärkeitä toimintoja.

Keskeistä on kansalaisten luottamus digitaalisiin palveluihin.

Kyberympäristö on paljon muuta kuin teknologiaa.

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

Kyber-maailma 2025?

Kiinalainen internet

BeiDou

Kiina
Baidu Tieba
WeChat
Youku Tudou
AliBaba
Nice, Meipai
Weibo
DidiKuaidi
C-trip
Alipay
Chinese Encyclopedia
Renren
QQMail/AliMail

China Net



President, Xi Jinping: **"We should respect the right of individual countries to independently choose their own path of cyber-development."** 2015

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

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

Venäläinen internet



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

Vuoden 2019 laki velvoittaa ohjaamaan kaiken internetliikenteen Venäjän Roskomnazorin hyväksymien tai sen itse hallitsemien solmujen läpi.

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

Venäjä testasi RuNetin irrottamista loppuvuodesta 2019, sanoen sen onnistuneet. Tätä ei ole voitu varmentaa.

Venäjän Uuden sukupolven sodankäynti

Laaja-alainen suora ja epäsuora vaikuttaminen fyysisessä ja virtuaalisessa toimintaympäristössä.

Jatkuva toiminta kybermaailmassa sodan kynnyksen alapuolella attribuution tavoittamattomissa.



Lähde: Bērziņš, J. (2019). Not 'Hybrid' but New Generation Warfare, kirjassa: Russia's Military Strategy and Doctrine (s.157-184)

Kyberpolitiikka ja -diplomatia

Niin kansallisessa kuin kansainvälisessä politiikassa painottuu yhä enemmän kyberasioiden poliittinen luonne (engl. Cyber Politics).

Kybertoimintaympäristöstä on tullut politiikan ja diplomatian kenttä ja se on voimakkaassa muutoksen tilassa.

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



Kyberpolitiikka ja -diplomatia

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


European Council
Council of the European Union

Search

Home > Press > Press releases

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

EU imposes the first ever sanctions against cyber-attacks

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

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

Kybervoima

Kybervoima/valta (Cyber Power = kybersuoritus kyvykkyydet vallankäytön välineinä) tulee määrittämään valtioiden roolin kybermaailmassa.

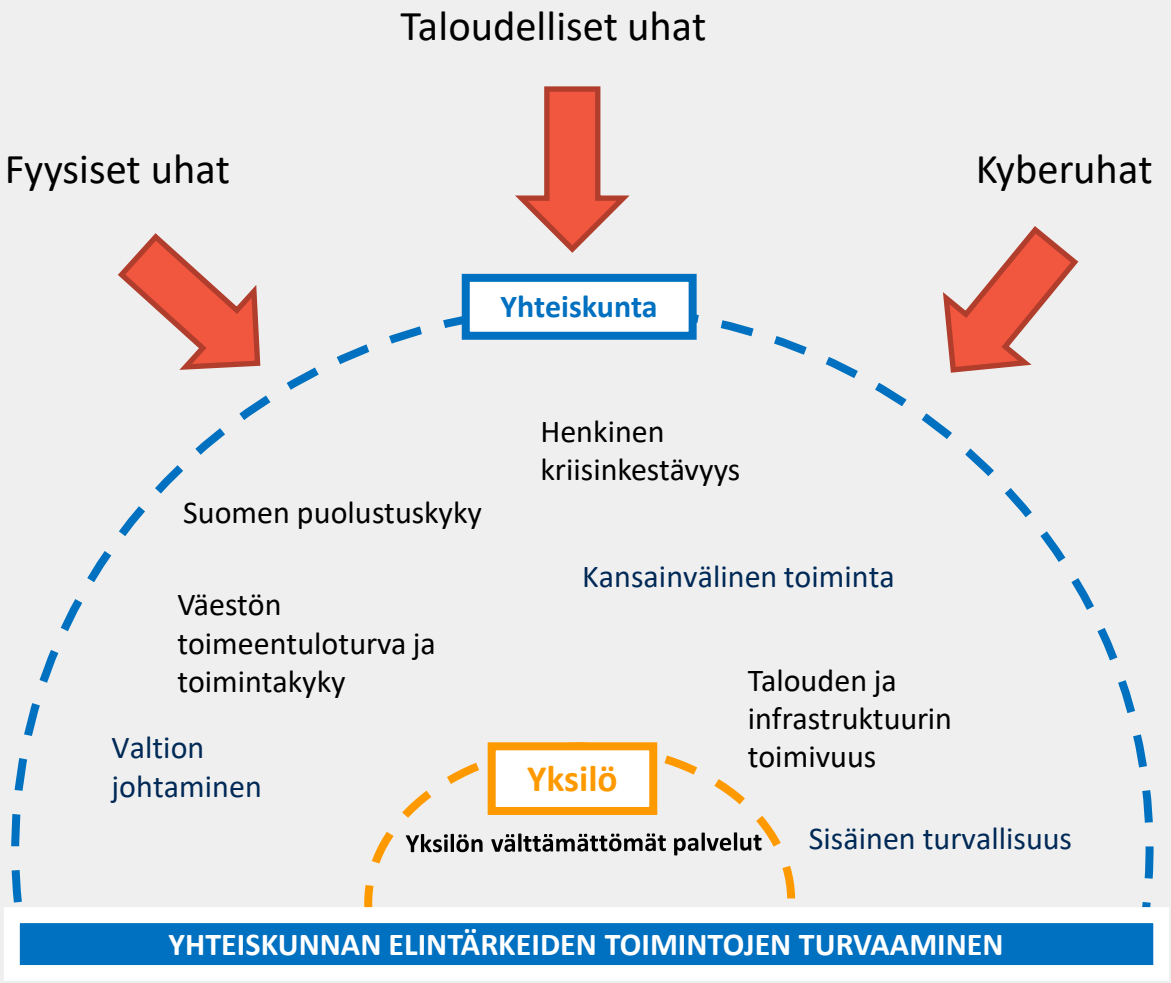
1. Kansallinen kyberympäristön valvontakyky,
2. Kansallinen kyberpuolustuskyky ja resilienssi,
3. Informaatioympäristön hallintakyky,
4. Laaja-alainen kybertiedustelukyky,
5. Kansallisen kyberteollisuuden suorituskyky,
6. Kyberhyökkäyskyky,
7. Kyberalan normien ja standardien määrittelykyky.

Suomen kansallista kybervoimaa/valtaa tulee kehittää edelleen.

Belfer Center
National Cyber Power Index 2020 "Top 10"

#	Country	Overall score
1	**United States**	50.24
2	**China**	41.47
3	**United Kingdom**	35.57
4	**Russia**	28.38
5	**Netherlands**	24.18
6	**France**	23.43
7	**Germany**	22.42
8	**Canada**	21.50
9	**Japan**	21.03
10	**Australia**	20.04

Yhteiskunnallinen ulottuvuus



Selonteko: ”Ukrainan tilanne on korostanut entisestään toimitusketjujen hallinnan merkitystä myös ohjelmistojen ja digitaalisten palveluiden osalta.”

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

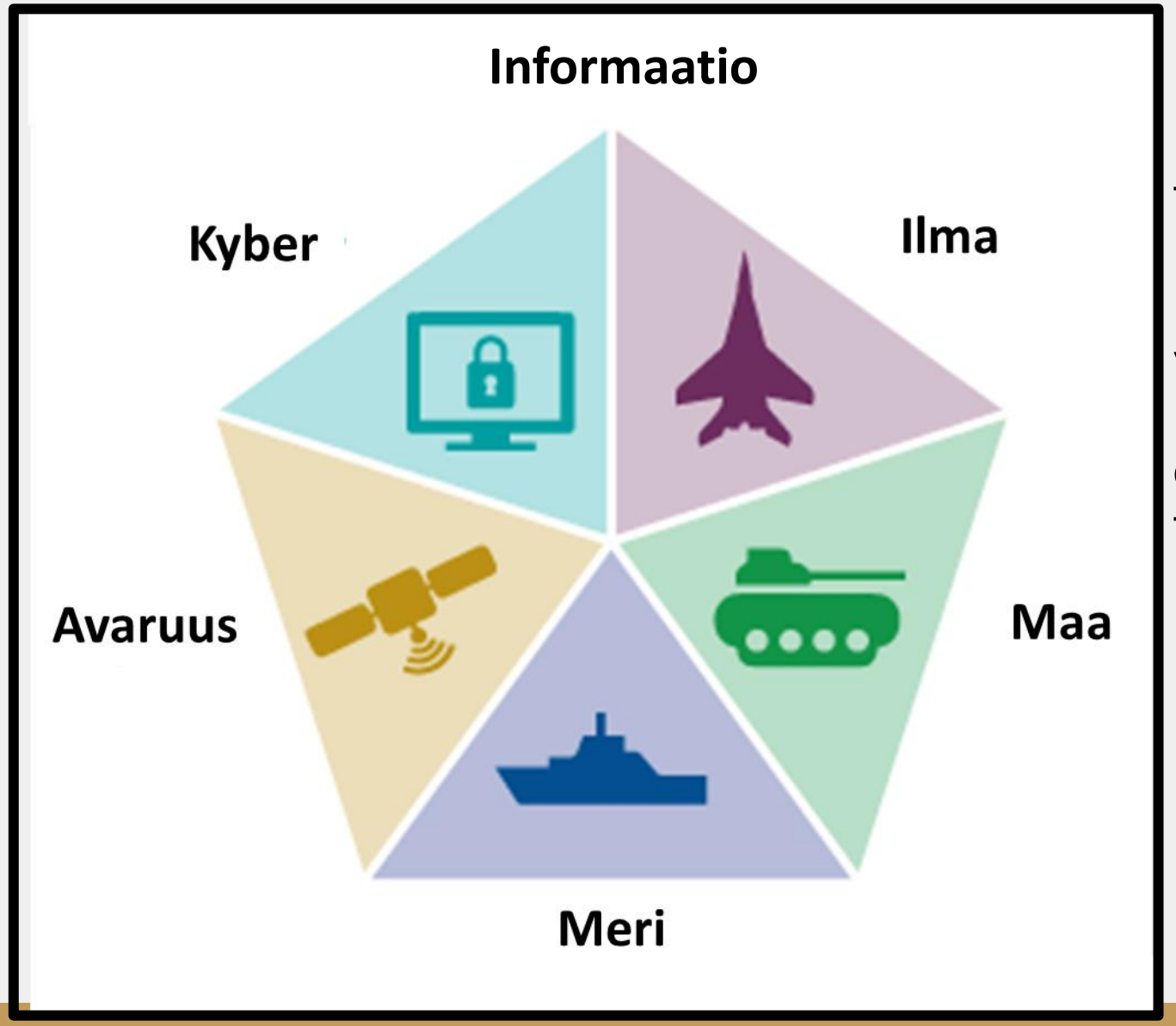
Yhteiskunnallinen ulottuvuus



NATO-prosessin aikana Venäjä voi kohdistaa toimia maamme kriittistä infrastruktuuria kohtaan aiheuttaakseen epävarmuutta ja epäluottamusta kansalaisissa sekä osoittaakseen valtiojohdolle kyvykkyytensä lamauttaa kriittisiä toimintoja.

Kyberpuolustus

Puolustusvalmiuteen kohdistuvat vaatimukset ulottuvat kyber- ja informaatio-ympäristöihin.



Kaikkia toimintaympäristöjä on kyettävä valvomaan, ja niissä on tarvittaessa voitava käynnistää puolustuksen edellyttämät toimenpiteet.


CYBER DEFENCE

NATO:n kyberpuolustus

Kyberpuolustus on osa NATO:n ydintehtävää, kollektiivista puolustusta.

- Omien verkkojen suojaaminen
- Kyberkyvykkyys eri operaatioissa
- Jäsenmaiden auttaminen
- Poliittinen vaikutusfoorumi

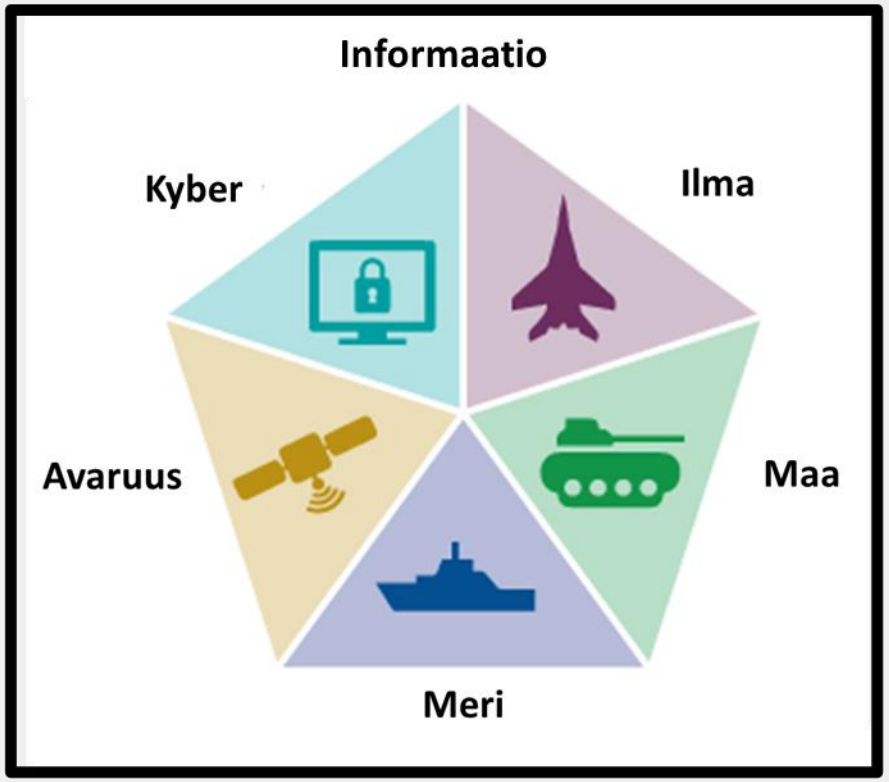
NATO:n lähtökohta on, että kukin maa vastaa omasta kyberpuolustuksestaan.



NATO-jäsenyys lisäisi mahdollisuutta kehittää kansallista suorituskykyämme ja samalla se velvoittaisi meitä huolehtimaan tehokkaasti omasta kyberpuolustuksestamme.

Kansallinen kybertila määriteltävä

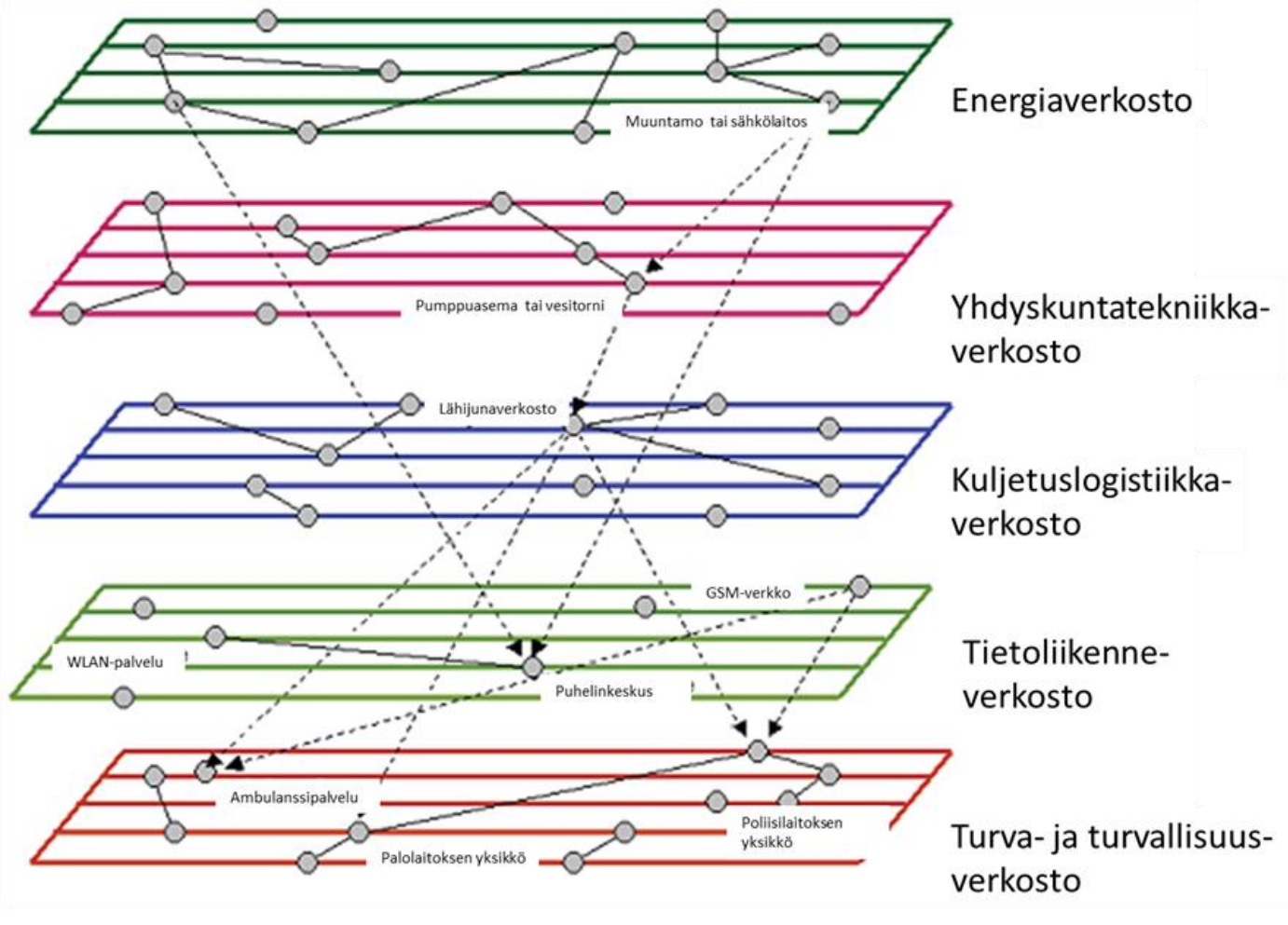
Aluevalvontalaki (18.8.2000/755) kuvaa Suomen valtakunnan aluetta määrittelemällä maa- ja merirajoja sekä niiden yläpuolista ilmatilaa.



AKV/AKT

Tavoitteena kansallinen suvereniteetti kybertilassa.

Kriittisen infrastruktuurin vahvistaminen



Tarvitaan sekä välittömiä että pitkä ajan toimenpiteitä.

1. Yritysten ja oppilaitosten osaamisen välitön käyttö.
2. Resurssointi osaamisen vahvistamiseen.

Kybervarautuminen

Jatkuvuuden hallinta

Häiriötilanteiden hallinta

Johtamisen ja kybertilannekuvan kehittäminen

Suomella tulee olla ajantasaisen kybertilannekuvan lisäksi selkeät johtamis- ja vastuusuhteet ja toimivaltuudet sekä kyvykkyys hyödyntää kaikkia yhteiskunnan voimavaroja.



Kansallista kybertilannetietoisuutta tulee kehittää suorituskykynäkökulmasta – kaikki hallinnolliset rajoitteet tulee voida ratkaista.

NATO-jäsenyys lisäisi kyberturvallisuutamme

NATO:n jäsenyys vahvistaisi kansallista kyberturvallisuutta, koska täysjäseninä olisimme oikeutettuja kaikkeen käytettävissä olevaan tietoon, voisimme osallistua puolustussuunnitteluun ja voisimme edelleen vahvistaa kybersuorituskykyämme.



Tarvitaan kyber/hybridinyrkki

Suomen NATO-prosessi aiheuttaa hyvin todennäköisesti vakavia toimenpiteitä Venäjän taholta.

Tässä tilanteessa tulisi koronanyrkin tavoin perustaa operatiivinen kyber/hybridinyrkki.

Tämän kriisiryhmän tehtävä olisi kartoittaa Suomeen kohdistuvat kyber/hybridiuhat ja haavoittuvuudet, vahvistaa tilannekuvan muodostamista ja ehdottaa tarvittavia toimenpiteitä sekä tukea häiriötilanteiden hallintaa.

Kokonaisturvallisuus

Kokonaisturvallisuuden toimintamalli tulee sovittaa nykyiseen turvallisuustilanteeseen.

Kansallinen kyberturvallisuus on keskeinen osa kokonaisturvallisuutta, johon meidän on kyettävä osallistamaan eri toimijat sekä yhteensovittamaan voimavarat ja toimintatavat mahdollisimman tehokkaasti asetettujen yhteiskunnan strategisten tavoitteiden saavuttamiseksi.



Kiitos

www.jyu.fi/it

