
DARKSOC®
JOHDATUSTA
KYBERTURVALLISUUTEEN
CYBERWATCH FINLAND

Pertti Jalasvirta, Partner/hallituksen puheenjohtaja Cyberwatch Oy

Kokemus

Johtoryhmä- ja hallitustasolla Suomessa ja kansainvälisesti

Kehittämisen suunnittelu

Turvallisuus Kenttäsairaaloiden kehittäminen, koulutuksen suunnittelu

CBRN-suojaus ja turvallisuus

Kansainvälinen harjoitustoiminta, strateginen kyberturvallisuus

Dark ja Deeb web

Analysointi ja tiedustelun tutkimus

Sosiaalifysiikan

Tutkimus ja kehittäminen

Associate Fellow, Geneve Centre For Security Policy, GCSP

Kansainvälinen puhuja

Tutkinnot:

Johtamisesta (Kybermaster), tuotekehityksestä, yrittäjyydestä ja media-alan johtamisesta (meneillään)

Julkaisut:

Knowledge mining of unstructured information, Implementing

RFID technology in a novel triage system during a simulated mass casualty situation.

Artikkelit

Project Aether – Air Passenger Transport Security in Case of CBRN Terrorism

Osaamisen kehittäminen

120 Kybermaster tutkinnon suorittajaa

Kyberturvallisuus

- **Tavoitetila** - > pyrkimys kybertoimintaympäristöön, johon voidaan luottaa ja jossa sen toiminta turvataan

- **Kyberturvallisuus** tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Kyberturvallisuuteen kuuluvat toimet, jotka ovat tarpeen verkko- ja tietojärjestelmien, järjestelmien käyttäjien ja muiden kyberuhkien kohteena olevien henkilöiden suojaamiseksi

- **Tietoturvalla** tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta. (kyberturvallisuuden-sanasto, turvallisuuskomitea)

MITÄ ON KYBERTURVALLISUUS

CYBERWATCH FINLAND

DARK, DEEP WEB, OSINT

NIIHIN LIITTYVIEN RISKIEN TUNNISTAMINEN

KESKINÄISRIIPPUVUUKSIEN HAVAINNOINTI

DARKSOC™ kyky perustuu oivallukseen ihmis- ja organisaatiosensorien määrästä – sensoreita on yhtä paljon, kuin maailmassa on internetiin kytkettyjä päätelaitteita.

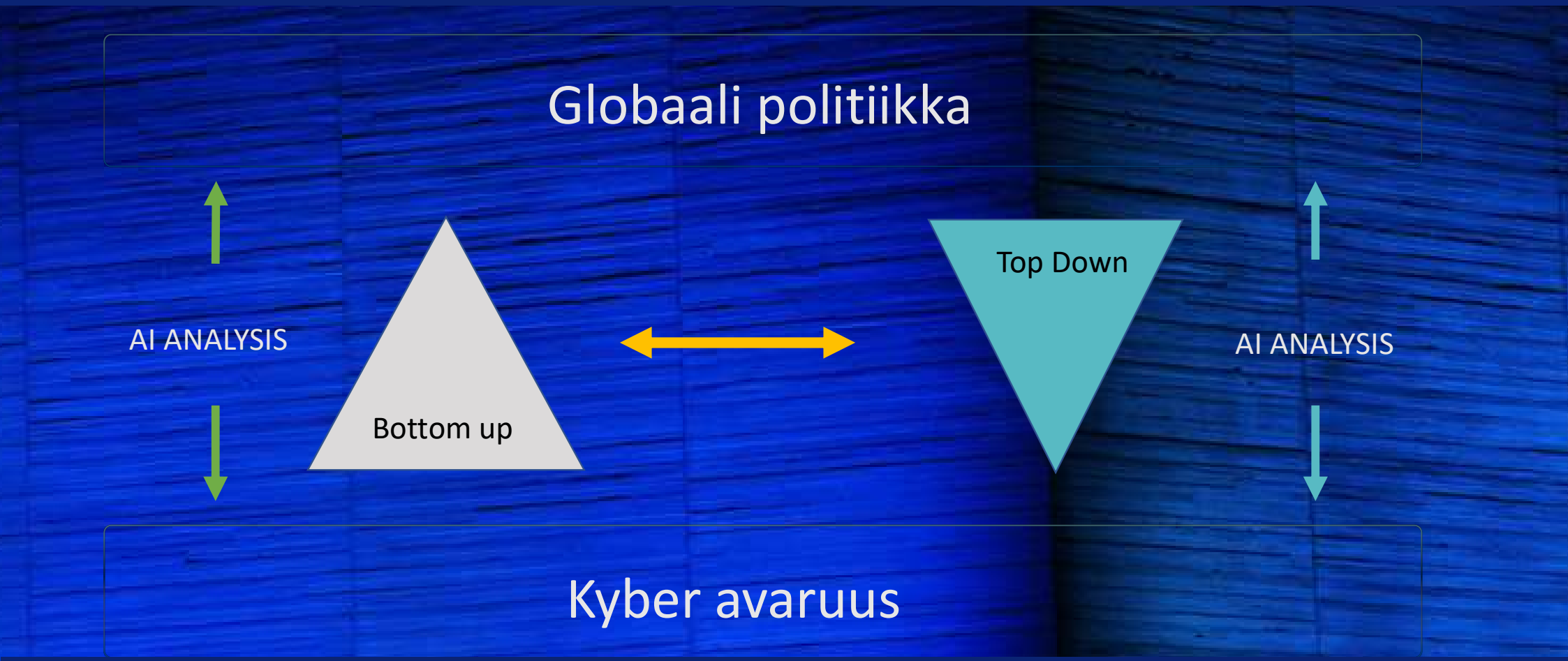
DARKSOC™ selvittää kohdennetusti organisaation sen hetkisen kybervalmiustilan, tuottaa riskianalyysin, sekä operatiiviset ja strategiset suositukset.

Se sisältää ennakoivat vaaratilanneilmoitukset, uhkatekijöiden mallinnuksen, avainkohteiden ja -henkilöiden uhka- ja riskianalyysit, sekä tiedon maalitetuista henkilöistä, toiminnoista ja organisaatioista.

DARKSOC™ perustuu tieteelliseen tutkimustyöhön, jota Cyberwatch Finland on tehnyt tutkimuslaitosten kanssa useita vuosia.

Lopputuloksena on kehitetty sosiaalisen fysiikan menetelmiä hyödyntävä algoritmi, jota sovelletaan internetin syväkerroksista löydetyn tiedon jalostamiseen ja analysointiin, organisaation riskien tunnistamiseen ja hallintaan, sekä strategisen tilannekuvan rakentamiseen.

STRATEGINEN KYBERANALYYSI



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
Wikipedia	Chinese Encyclopedia	Big Russian Encyclopedia
Facebook	Renren	Vkontakte, Odnoklassniki
Gmail/Hotmail/Yahoo	QQMail/AliMail	Mail.ru
Internet	China Net	RuNet

Tulevaisuuden digitaalinen toimintaympäristö

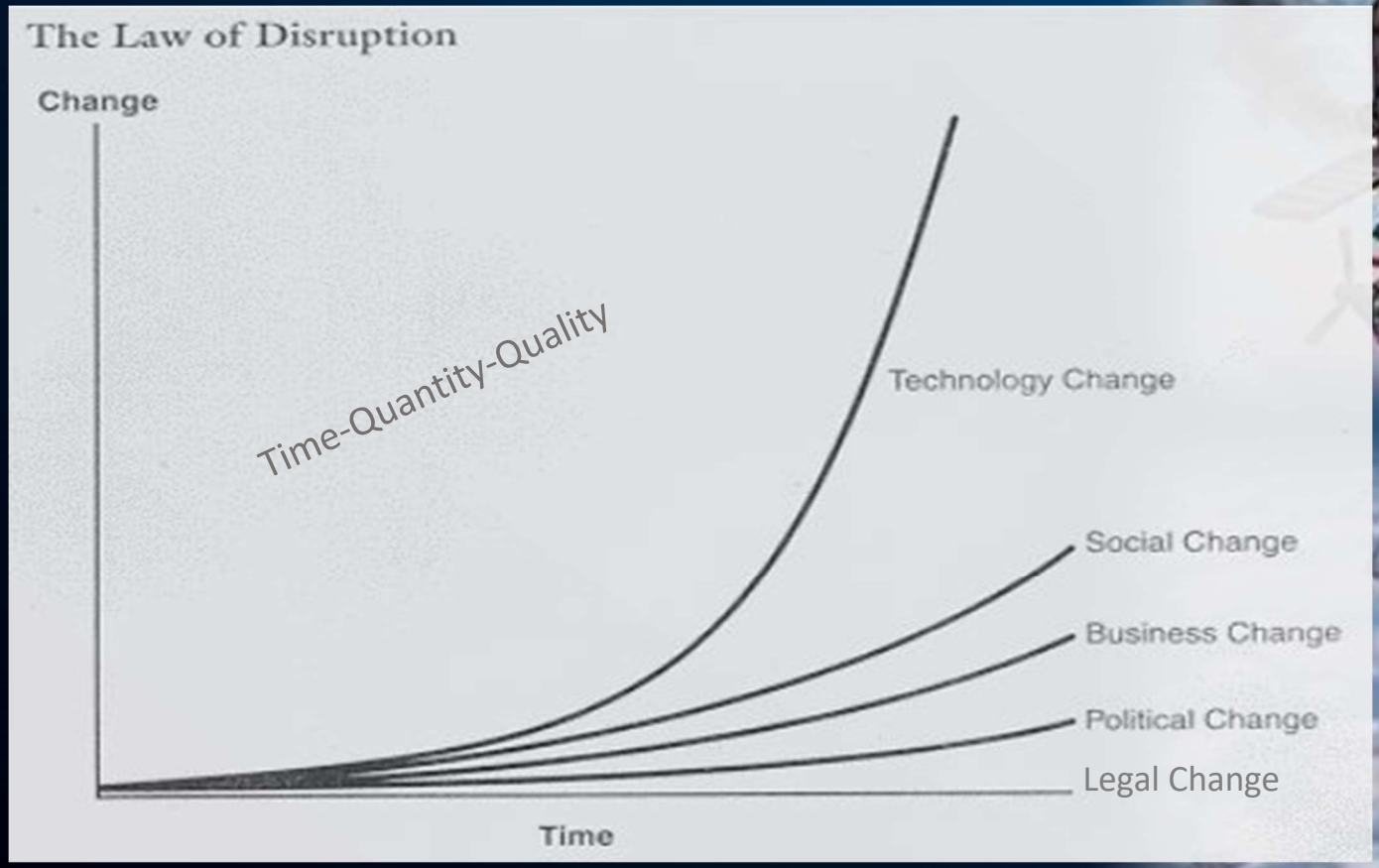
Digitaalinen kybertoimintaympäristö on voimakkaasti politisoitunut.

Suurvallat haluavat luoda oman verkon, jota voivat hallita ja valvoa.

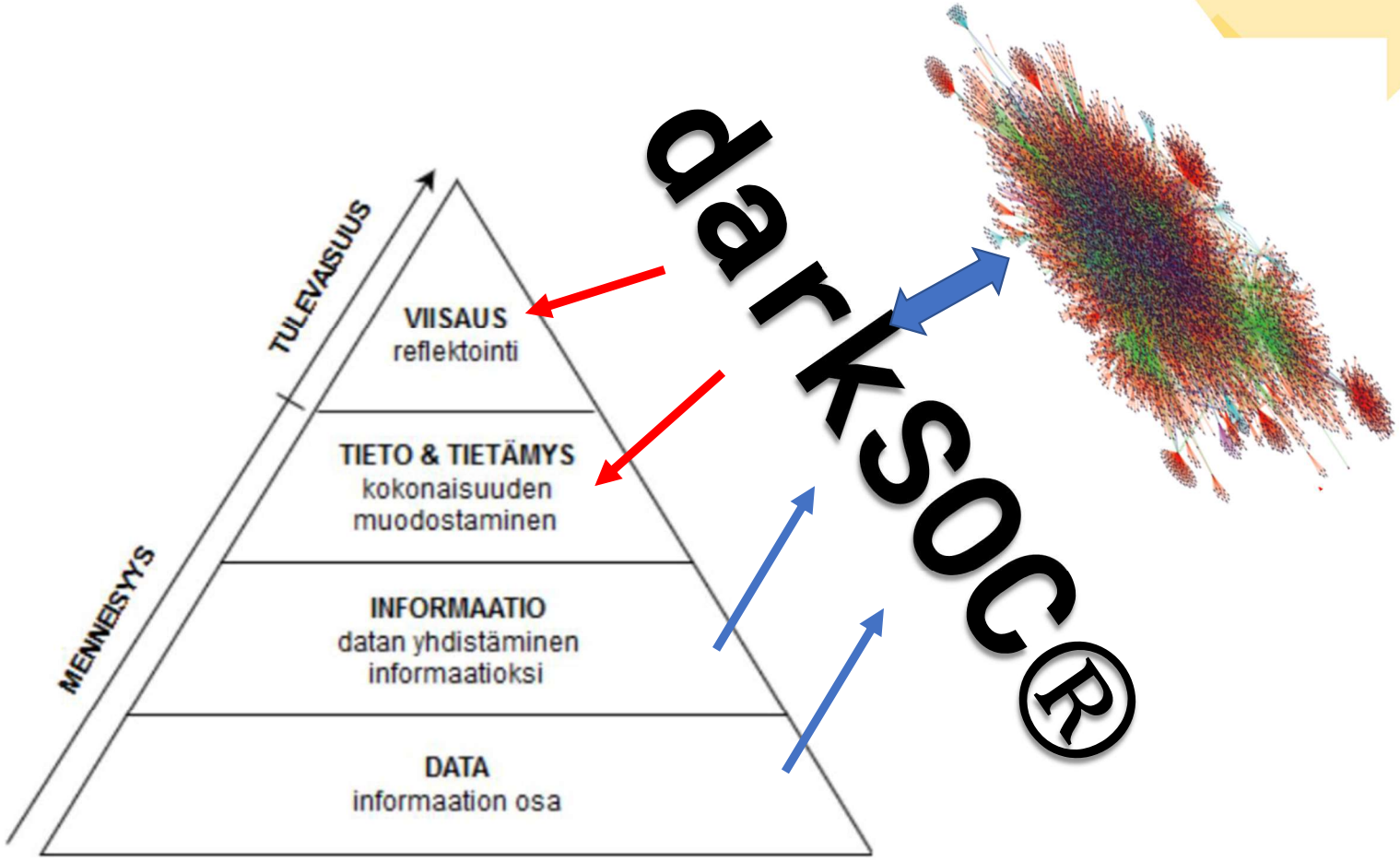
Kansainväliseen politiikkaan on tullut käsitteet:

- kyberpolitiikka (Cyber policy)
- kyberdiplomatia (Cyber diplomacy)
- kybervoima (Cyber power)
- Kybersodankäynti (fyysisen sodan yhteydessä).
- kyberoperaatio (ei sotatilaa)

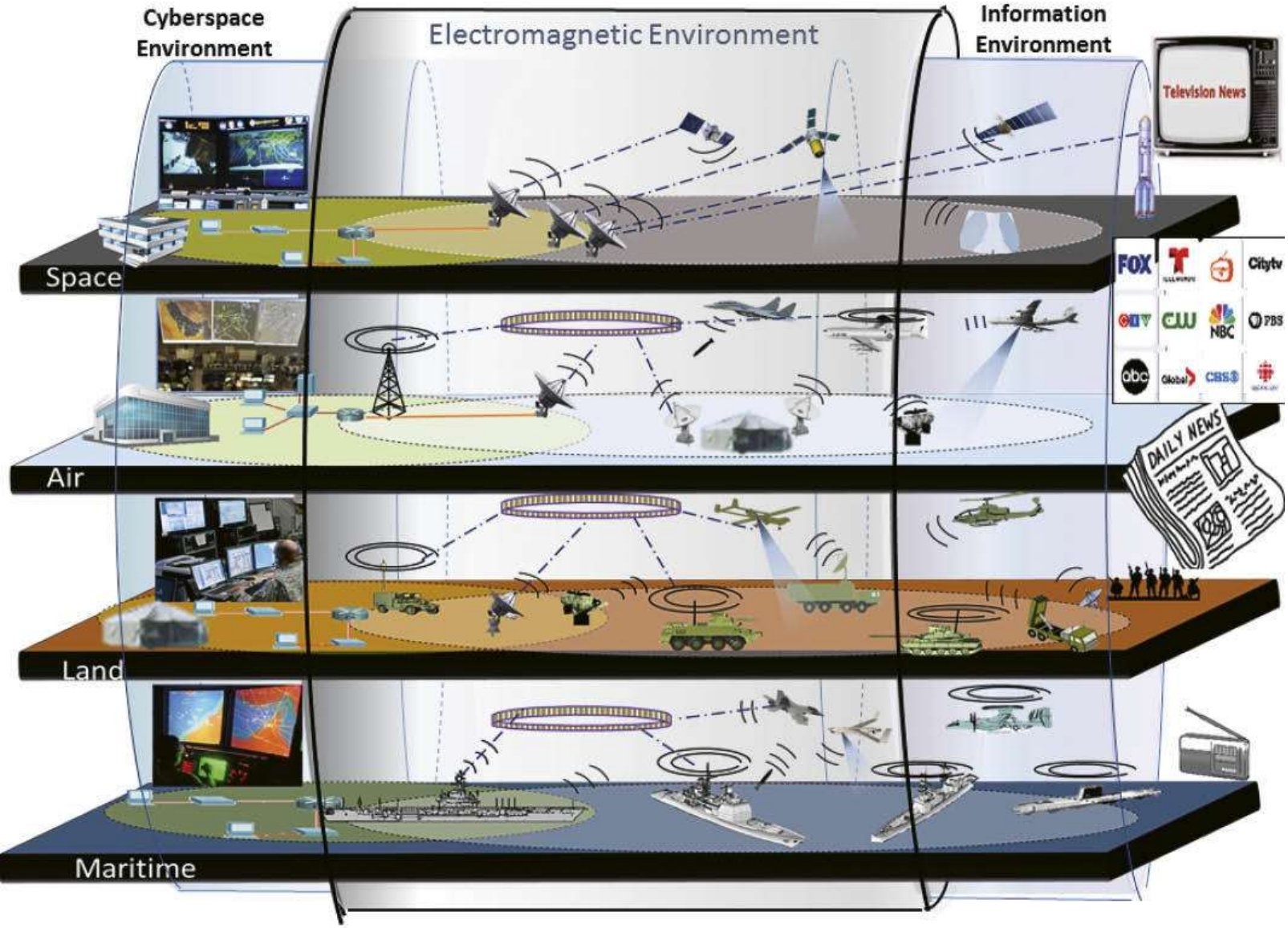
Dystopia: **From history to the future**



TIEDON TASOT



Kuva 1. Datasta viisauteen (mukaillen Ritholtz, 2010).

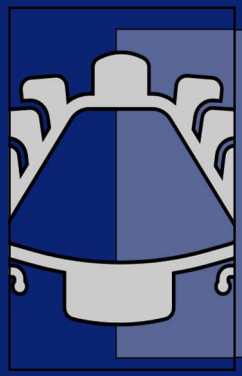


Digitaalinen toimintaympäristö

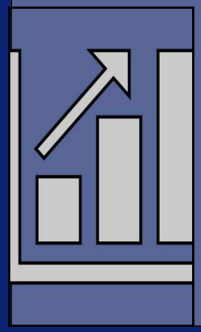
Kyber, sähkömagneettinen spektri ja informaatioympäristö muodostavat uuden digitaalisen ja keskinäisriippuvan toimintaympäristön.

Häiriöt ja hyökkäysoperaatiot vaikuttavat näiden ympäristöjen välillä, koska ne ovat tiiviisti verkottuneet keskenään.

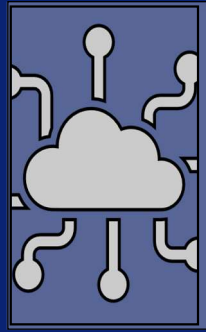
Kriittisen infrastruktuurin kolme ulottuvuutta



Poliittinen ulottuvuus käsittää kansallinen lainsäädäntö ja kansalliset turvallisuustarpeet sekä kansainvälinen yhteistyö näiden ympärillä.

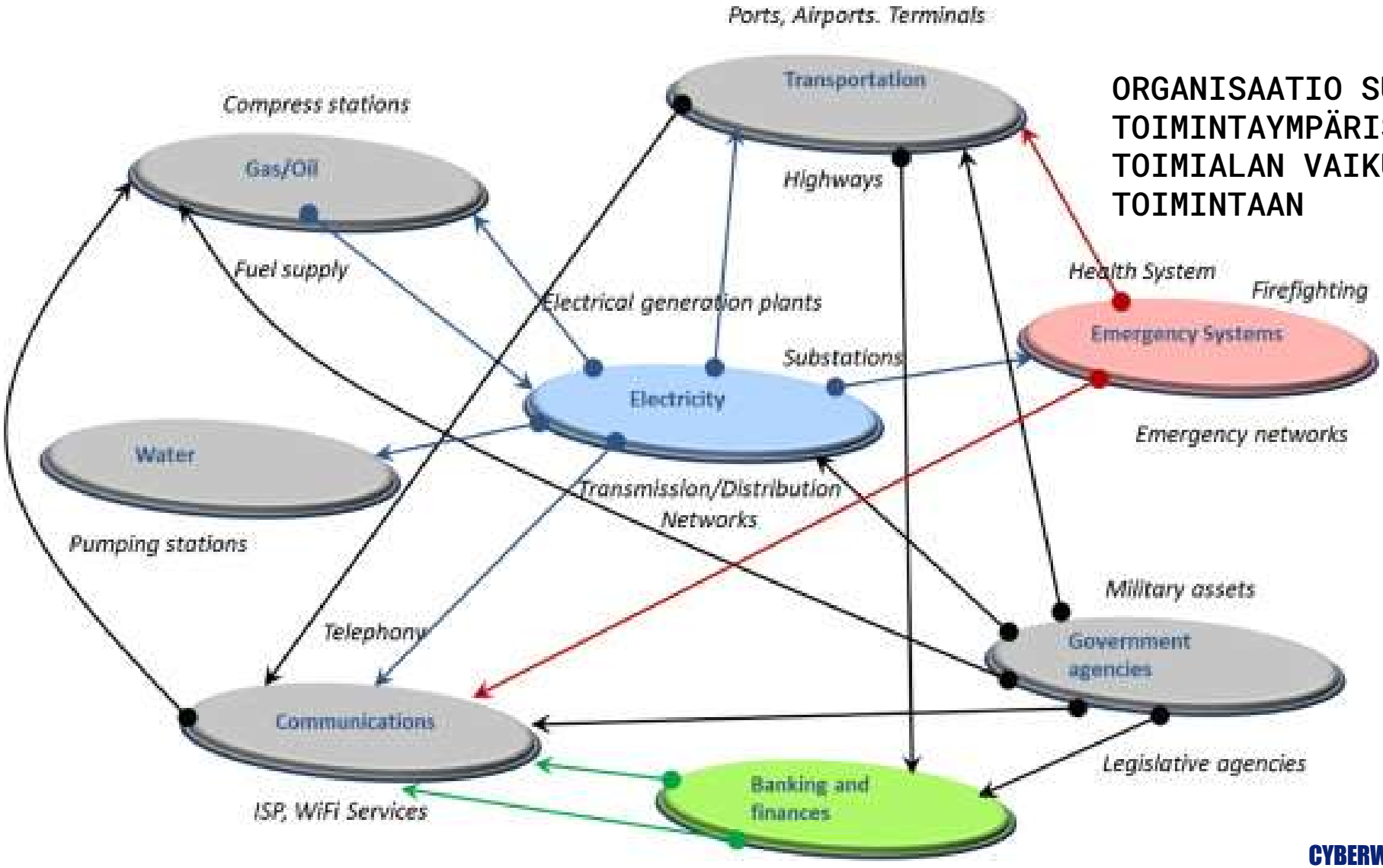


Taloudellinen ulottuvuus käsittää kaikki ne yritykset ja muut taloudelliset toimijat, jotka rakentavat, omistavat ja hallinnoivat infrastruktuurijärjestelmiä ja -laitoksia ja jotka toimivat taloudellisten intressien mukaisesti.



Teknologinen ulottuvuus käsittää sen hyödyntämisen sekä kaikki ne käytännön ratkaisut ja toimenpiteet, joita valtiot ja yritykset tekevät turvatakseen kriittisen infrastruktuurinsa toimivuutta mahdollisten häiriöiden varalta.

ORGANISAATIO SUHTEESSA TOIMINTAYMPÄRISTÖÖN JA TOIMIALAN VAIKUTUKSET TOIMINTAAN



CYBERWATCH FINLAND

Cyberspace Operation – Motivation?

Cyber warfare

Cyber sabotage

Cyber terrorism

Cyber espionage

Cyber-crime

Cyber vandalism

Attack to paralyze the function vital to society

Attack to disrupt the function vital to society

Attack to create chaos in society

Attack to hide actual cyber espionage attack

Attack to get money (ransoms)

Attack to harm the organization

DDOS-attack motivation

Kyberkapasiteetin kehittäminen (cyber capasity building, CCB)

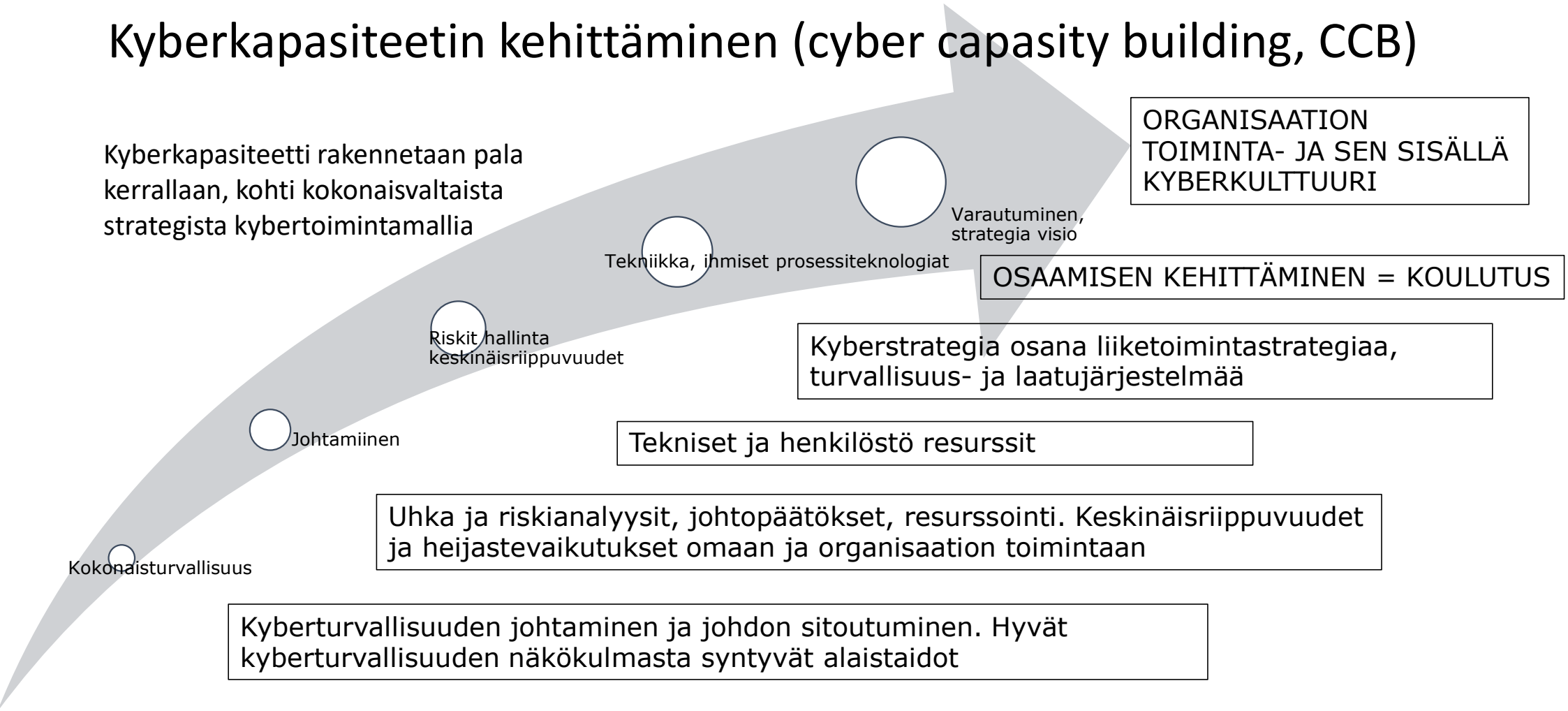
Kyberkapasiteetin kehittämisen ensisijaisena tavoitteena on **vähentää haitallisen toiminnan riskiä ja siten myös kustannuksia kybertoimintaympäristössä.**

Tämä edellyttää kansallisten ja organisaatiotason valmiuksien kehittämistä kyberhäiriöiden **ehkäisemiseksi, havaitsemiseksi ja käsittelemiseksi**.

Uhkana on haittaohjelmien käyttö laittoman pääsyn saamiseksi verkkoihin tietojen varastamiseksi tai sabotoimiseksi.

Rikolliset ja/tai valtiolliset toimijat voivat varastaa arkaluonteisia tietoja taloudellisen hyödyn saamiseksi tai hyökätä kriittiseen kansalliseen infrastruktuuriin (esim. televiestintäinfrastruktuuriin, sähköverkkoihin tai rahoitusmarkkinoihin) aiheuttaakseen laajoja häiriöitä sekä hämmentääkseen poliittista tilannetta kohdemaassa.

Kyberkapasiteetin kehittäminen (cyber capasity building, CCB)



CYBERWATCH FINLAND

Kybersodankäynnin käsite

OECD:n vuoden 2011 raportin mukaan kybersotaan liittyy samat sotilasdoktriinit kuin ns. tavalliseen sotaankin: kosto ja pelote.

Tutkijat yhtyvät käsitykseen siitä, että kybersodankäynnin määrittelyn tulisi perustua sodan tavoitteisiin ja motiiveihin eikä niinkään kyberoperaatioiden muotoihin.

Heidän mielestään sota on aina muodoltaan laaja-alainen käsittäen kaikki sodankäynnin muodot, jolloin kybersota on yksi sodankäynnin muoto, jota käytetään perinteisen kineettisen vaikuttamisen rinnalla.

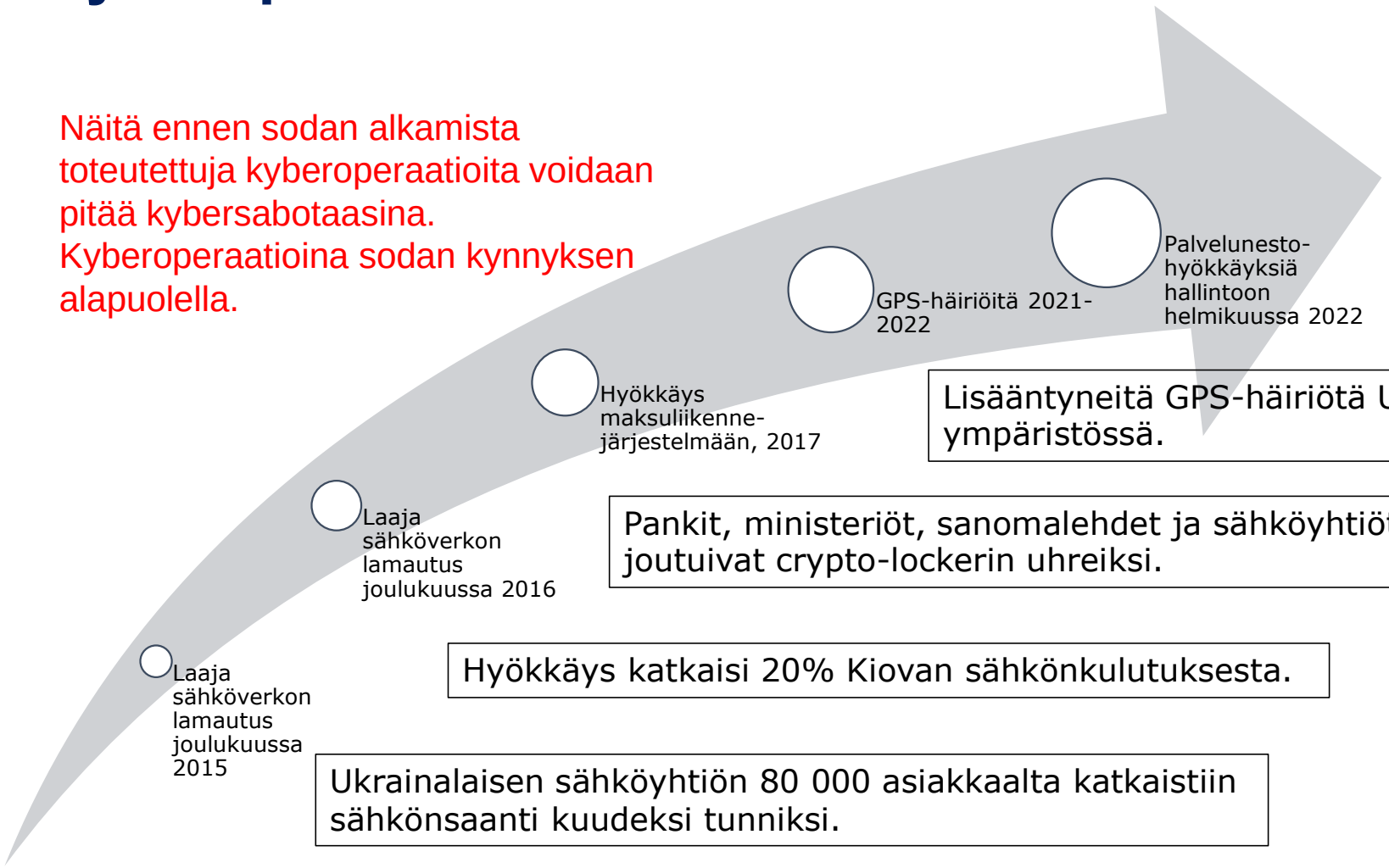
Kybersodankäynnin tasot ja näiden heijastevaikutuksiin varautuminen

- Kybersodankäynnin strategisen tason kyberoperaatioissa valtio pyrkii vaikuttamaan toisen valtion toimintaan sekä toimintakykyyn. Operatiivisella ja taktisella tasolla kyberoperaatioita suoritetaan osana muuta sotilaallista voimankäyttöä. Tavoitteena voi esimerkiksi olla sotilaallisen johtamisen häiritseminen, lamauttaminen tai harhauttaminen tai sotilaallisen voimankäytön estäminen tai viivästyttäminen.

- Kybersodan operatiivisella ja taktisella tasolla kysymys on kyberoperaatioista osana yhteisoperaatioita, joissa toimenpiteet kohdistuvat ensisijaisesti joukkojen johtamisjärjestelmiin. Näillä kyberoperaatioilla pyritään lamauttamaan vastustajan joukkojen tilannetietoisuuden muodostaminen sekä kyky tehokkaaseen joukkojen ja toiminnan johtamiseen.

Kyberoperaatioita Ukrainassa ennen 24.2.2022

Näitä ennen sodan alkamista toteutettuja kyberoperaatioita voidaan pitää kybersabotaasina. Kyberoperaatioina sodan kynnyksen alapuolella.



Laaja sähköverkon lamautus joulukuussa 2015

Ukrainalaisen sähköyhtiön 80 000 asiakkaalta katkaistiin sähkönsaanti kuudeksi tunniksi.

Laaja sähköverkon lamautus joulukuussa 2016

Hyökkäys katkaisi 20% Kiovan sähkönkulutuksesta.

Hyökkäys maksuliikenne-järjestelmään, 2017

Pankit, ministeriöt, sanomalehdet ja sähköyhtiöt joutuivat crypto-lockerin uhreiksi.

GPS-häiriöitä 2021-2022

Lisääntyneitä GPS-häiriötä Ukrainassa ja sen ympäristössä.

Palvelunesto-hyökkäyksiä hallintoon helmikuussa 2022

Kohteina ulko-, hätätila-, opetus- ja puolustusministeriö, asevoimat, pankkeja

CYBERWATCH FINLAND

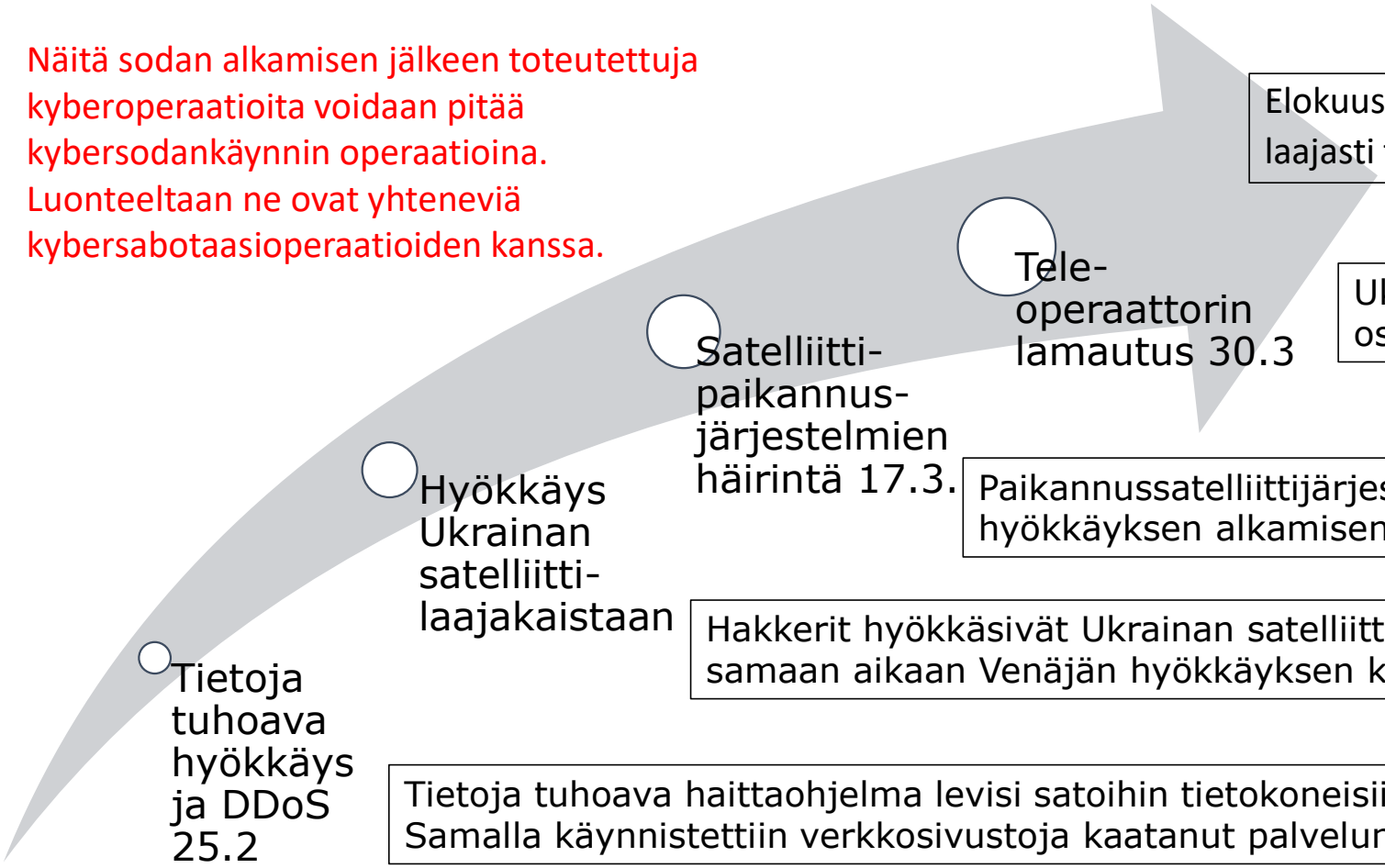
Venäjän toiminnan heikko vaikuttavuus

Mahdollisia syitä heikkoon tulokseen:

- Venäjä on käyttämät proxit eivät ehkä olleet huippuosaajia tämän tyyppisissä hyökkäyksissä
- Kyberhyökkäysten koordinointi ja johtaminen toteutettu huonosti
- Lännen avulla jo syksyllä 2021 voitiin Ukrainan kriittinen infrastruktuuri ”puhdistaa” mahdollisista takaovista ja tappokytkimistä
- Kaikkea hyökkäyskyvykkyyttä ei ole haluttu käyttää – jotain jäänyt takataskuun

Kyberoperaatioita Ukrainassa 24.2.2022 jälkeen

Näitä sodan alkamisen jälkeen toteutettuja kyberoperaatioita voidaan pitää kybersodankäynnin operaatioina. Luonteeltaan ne ovat yhteneviä kybersabotaasioperaatioiden kanssa.



Tietoja tuhoava hyökkäys ja DDoS 25.2

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

Hyökkäys Ukrainan satelliitti-laajakaistaan

Hakkerit hyökkäsivät Ukrainan satelliittilaajakaistaan samaan aikaan Venäjän hyökkäyksen kanssa.

Satelliitti-paikannus-järjestelmien häirintä 17.3.

Paikannussatelliittijärjestelmiä on häiritty Venäjän hyökkäyksen alkamisen jälkeen neljällä eri vyöhykkeellä.

Tele-operaattorin lamautus 30.3

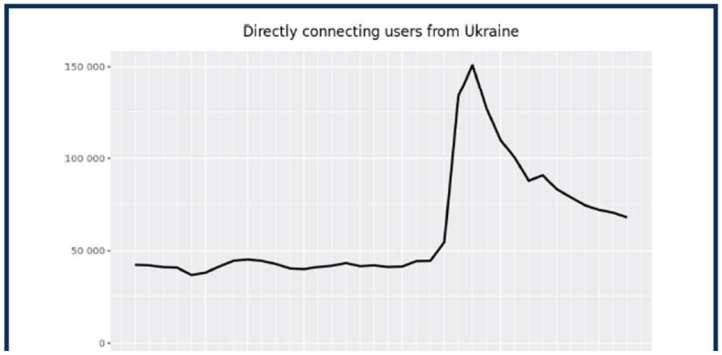
Ukrtelecomin yhteydet lamautuivat osin yli 15 tuntia.

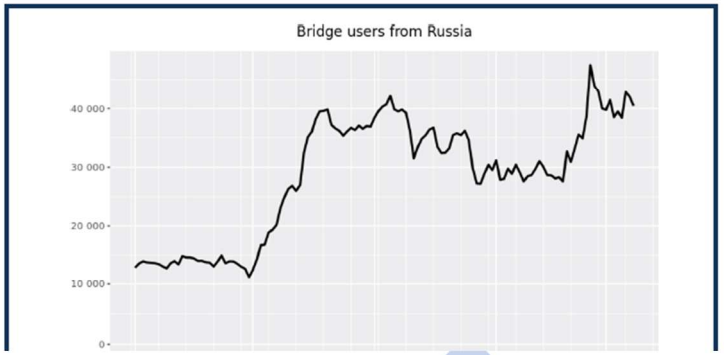
Elokuussa 2022 on aloitettu keräämään laajasti tiedustelutietoa kybertyökaluilla

DARKWEB TRENDS

- **RUSSIA: users have been connecting since late last year through the node bridges.**
- **There was a huge spike at the start of the war from Ukraine.**
  - The decrease afterwards is due to electrical blackouts and people fleeing the war.
- **When censorship starts, people will continue to look for objective information with the help of TOR.**

Pro-Russian Trends





DARKSOC®
Määrällinen, laadullinen ja ajallinen altistuminen.

CYBERWATCH FINLAND

Lost data sold on Dark and Deep web marketplaces and at affordable prices

Product	Avg. Price USD (2020)	Avg. Price USD (2021)	YoY Difference
Cloned Mastercard with PIN	$15	$25	+$10
Cloned American Express with PIN	$35	$35	$0
Cloned VISA with PIN	$25	$25	$0
Credit card details, account balance up to $1,000	$12	$15	+$3
Credit card details, account balance up to $5,000	$20	$24	+$4
Stolen online banking logins, minimum $100 on account	$35	$40	+$5
Stolen online banking logins, minimum $2,000 on account	$65	$120	+$55
Walmart account with credit card attached	$10	$14	+$4

Lost data sold on Dark and Deep web marketplaces and at affordable prices

Social Media	Avg. Price USD (2020)	Avg. Price USD (2021)	YoY Difference
Hacked Facebook account	$75	$65	-$10
Hacked Instagram account	$55	$45	-$10
Hacked Twitter account	$49	$35	-$14
Hacked Gmail account	$156	$80	-$76
Instagram followers x 1000	$7	$5	-$2
Spotify followers x 1000	$3	$2	-$1
Twitch followers x 1000	$6	$5	-$1
LinkedIn x 1000	$10	$12	+$2
Pinterest followers x 1000	$5	$4	-$1
Soundcloud plays x 1000	$1	$1	$0
Twitter retweets x 1000	$25	$25	$0
Instagram likes x 1000	$6	$5	-$1

France Passport	$4,000
Lithuanian passport	$1,500
Maltese Passport	$6,500
Maltese Passport	$6,500
Various European Union passports	$4,000

There is no need to develop attack programs, ready-made ones are available in marketplaces

Malware	Avg. Price USD (2020)	Avg. Price USD (2021)	YoY Difference
Global low quality, slow speed, low success rate x 1000	$70	$50	-$20
Europe low quality, slow speed, low success rate x 1000	$300	$320	+$20
USA, CA, UK, AU low quality, slow speed, low success rate x 1000	$800	$900	+$100
Global med quality, 70% success rate x 1000	$80	$80	–
Europe med quality, 70% success rate x 1000	$700	$500	-$200
USA only med quality, 70% success rate x 1000	$900	$1,000	+$100
USA, CA, UK, AU med quality, 70% success rate x 1000	$1,300	$1,400	+$100
Europe fresh high quality x 1000	$2,300	$2,500	+$200
Europe aged high quality x 1000	$1,400	$1,200	-$200
USA high quality x 1000	$1,700	$1,900	+$200
CA high quality x 1000	$1,500	$1,400	-$100
UK high quality x 1000	$2,000	$2,200	+$200
Android x 1000	$600	$900	+$300
Premium x 1000	$6,000	$5,000	-$1,000

DDOS Attacks	Avg. Price USD (2020)	Avg. Price USD (2021)	YoY Difference
Unprotected website, 10-50k requests per second, 1 hour	$10	$15	+$5
Unprotected website, 10-50k requests per second, 24 hours	$60	$50	-$10
Unprotected website, 10-50k requests per second, 1 week	$400	$500	+$100
Unprotected website, 10-50k requests per second, 1 month	$800	$1,000	+$200
Premium protected website, 20-50k requests per second, multiple elite proxies, 24 hours	$200	$200	–

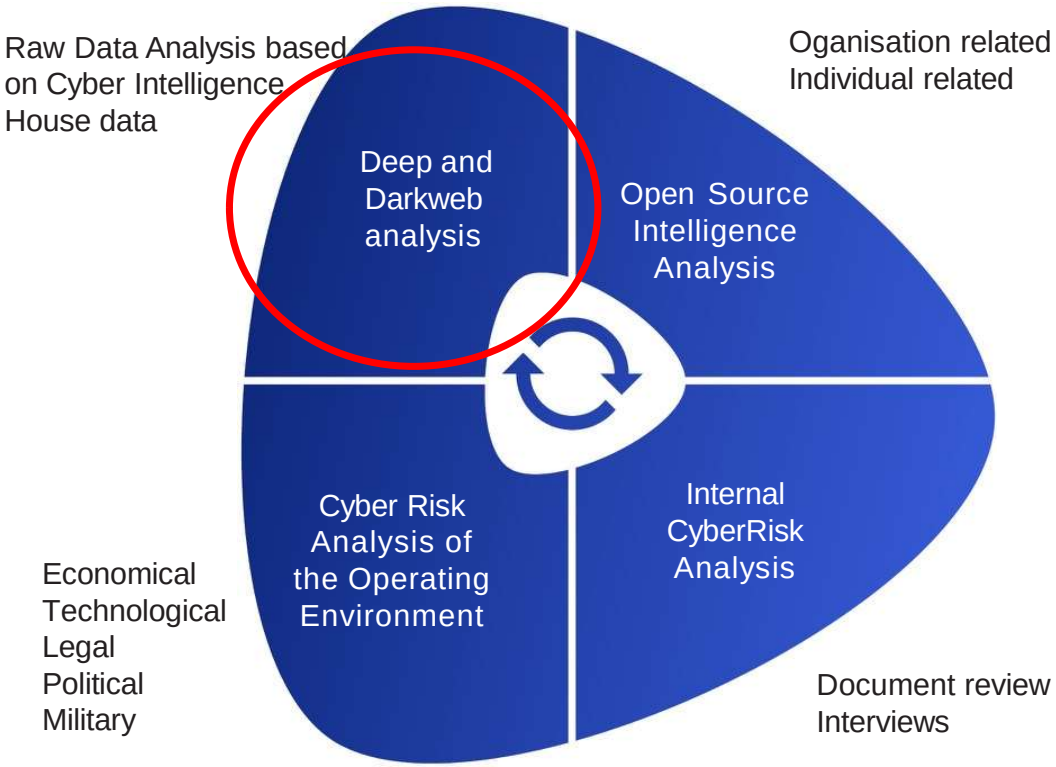
DARKSOC® -AS A SERVICE

DARKSOC® on Cyberwatch Finlandin kehittämä modulaarinen palvelu, joka analysoi organisaation nykyisen kyberturvallisuusympäristön, selvittää mahdolliset ongelma-alueet digitaalisen jalanjälkesi selvittämiseksi. Tämän avulla yhtiö voi reagoida varoituksiin ja ymmärtää motiiveja, sekä syitä hyökkäysten takana

Palvelun raportointi nopeuttaa reagointikykyä ja parantaa kykyä tehdä operatiivisia ja strategisia päätöksiä oikea-aikaisesti.

Tietoja kerätään useista eri lähteistä. Kerätyistä ja validoiduista tiedoista analyytikot tuottavat raportin, jonka perusteella ymmärretään havaintojen merkitys ja arvo oman organisaatiosi päätöksenteon näkökulmasta.

Raakadatan louhintaan **DARKSOC® -**palveluna käyttää yhtenä tietolähteenä Cyber Intelligence Housen tietokantoja ja palvelimia, jotka sijaitsevat ympäri maailmaa ja keräävät tietoja yhdeksän gigabitillä sekunnissa reaaliajassa.



1. LÄHESTYMISTAPAMME

KUINKA TEEMME SEN?

- valitsemalla avainsanat yhdessä kanssasi
- sopimalla tavoitteista eri vaiheille
- hakemalla luokiteltuja raakatietoja järjestelmästä
- tekemällä nykytilan analyysi
- sopimalla välittömistä lisätoimista ja kehittämistoimenpiteistä
- seuraamalla jatkuvasti toimenpiteiden vaikutusta ja tehokkuutta näkyvyyteesi syvässä ja pimeässä verkossa

JOHDANTO: MITEN ALTISTUTAAN?

Luokittelemme kyberaltistumisen vaikutukset kahdeksaan kategoriaan.

Kyberaltistuminen määritellään haavoittuvuuksiksi, joita syntyy, kun käytämme tietokonetta tai muuta digitaalista laitetta verkkotekniikan kanssa.

Jokainen yksittäinenkin vuotanut tieto on kriittinen.

TIETOSUOJA

Tekninen turvallisuus

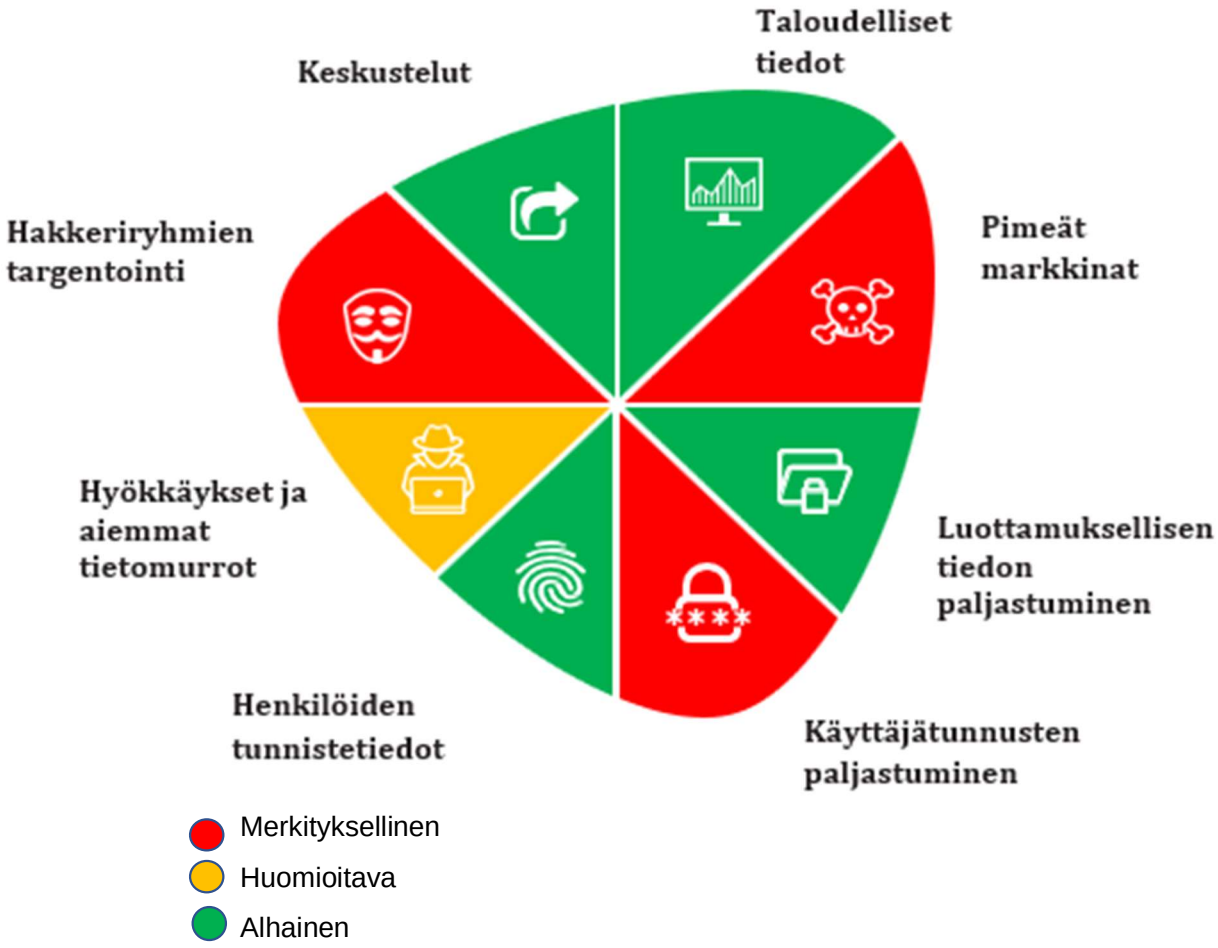
Pääsy tietoihin vaatii vahvan tunnistautumisen ja on rajoitettu vain valtuutetuille Cyberwatch Finlandin työntekijöille.
Kaikki kirjautumiset tunnistetaan ja niitä valvotaan.
Sisäinen ja ulkoinen viestintä hoidetaan suojatulla tai salatulla järjestelmällä.

Organisaation turvallisuus

Palvelulle on toteutettu tietosuojan vaikutustenarviointi.
Kaikki Cyberwatch Finlandin työntekijät ja johto ovat velvollisia käsittelemään henkilötietoja luottamuksellisina.
Tietojen saatavuus on rajoitettu valituille työntekijöille.
Vain toimeksiannon kannalta merkityksellisiä tietoja käsitellään. Erityisiä henkilötietoja ei käsitellä.

KESKEISET HAVAINNOT ESIMERKKI

- Asiakkaan osalta merkittävimmät havainnot liittyivät yleensä myynnissä olevaan tietoon, vuotaneisiin käyttäjätunnuksiin sekä hakkeriryhmien targetointiin.
- Saatavilla oleva asiakkaaseen liittyvän tiedon määrä on yleensä merkittävä ja tämä vaikuttaa suoraan kohonneeseen kyberriskiin.
- Merkittävää on, että moni altistumista osoittava kuvaaja on yleensä selkeästi noussut verrattuna vuoden takaiseen havaintojen määrään. Oikeilla toimenpiteillä saadaan altistumiset tasaantumaan
- Analysoitava yhdessä organisaation verkoston kanssa muodostavat suuren kokonaisuuden ja sen vuoksi hyökkäyspinta-ala on yleensä varsin laaja.
- Yhdistämällä tähän SOC data ja muu sisäinen tieto luodaan kykyä ja viisautta ymmärtää asioiden keskinäisriippuvuuksia, sekä luodaan ennakointi kykyä ja allokoidaan resursseja tulevaan.



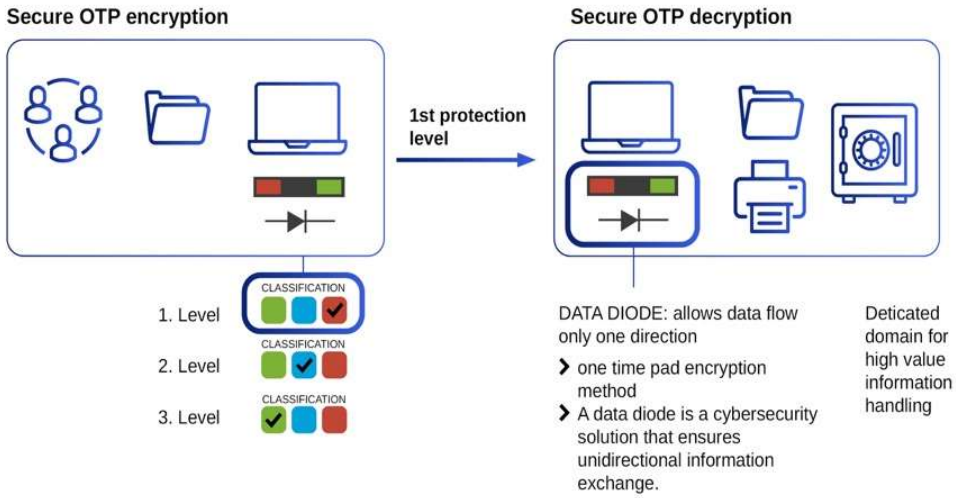
RAPORTIN TOIMITTAMINEN

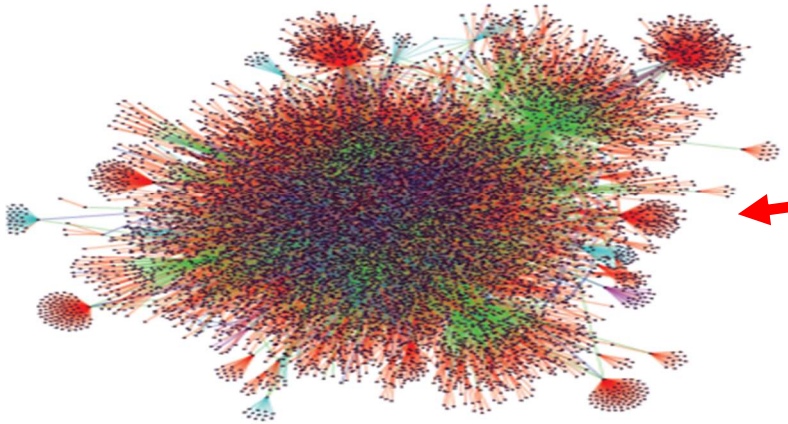
Kirjallinen raportti toimitetaan lähtökohtaisesti turvapostilla (TL IV-taso).

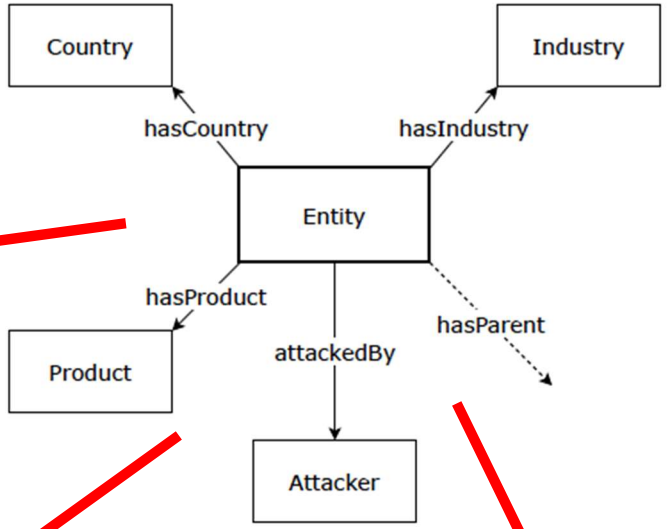
Tarvittaessa toimitus voidaan tehdä myös eri korvausta vastaan salatulla datadiodilla (TL II-taso).

Yksisuuntainen verkko (kutsutaan myös yksisuuntaiseksi yhdyskäytäväksi tai datadiodiksi) on verkkolaite tai laite, joka sallii tiedon kulkemisen vain yhteen suuntaan.

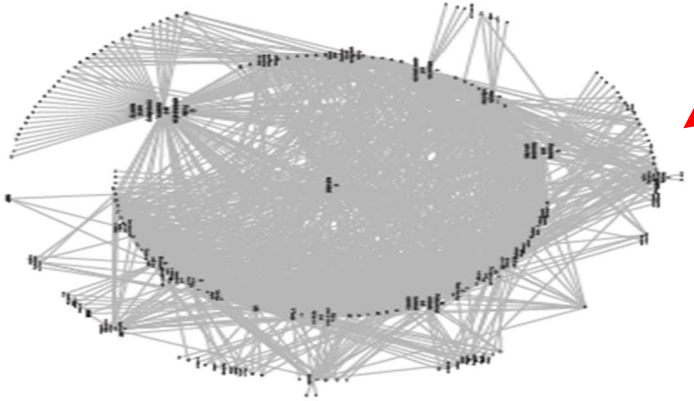
Datadiodit löytyvät yleisimmin korkean turvatason ympäristöistä, joissa ne toimivat yhteyksinä kahden tai useamman eri turvallisuusluokituksen omaavan verkon välillä.

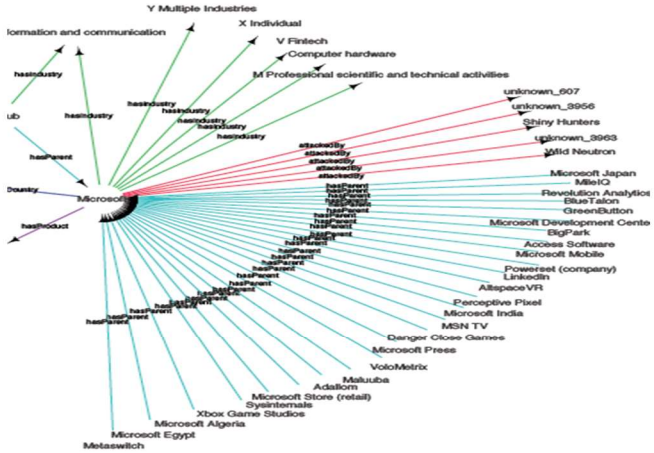






DBpedia	Study
foaf:name	Name
dbo:industry	hasIndustry
dbp:locationCountry	hasCountry
dbo:product	hasProduct
dbo:parentCompany	hasParent

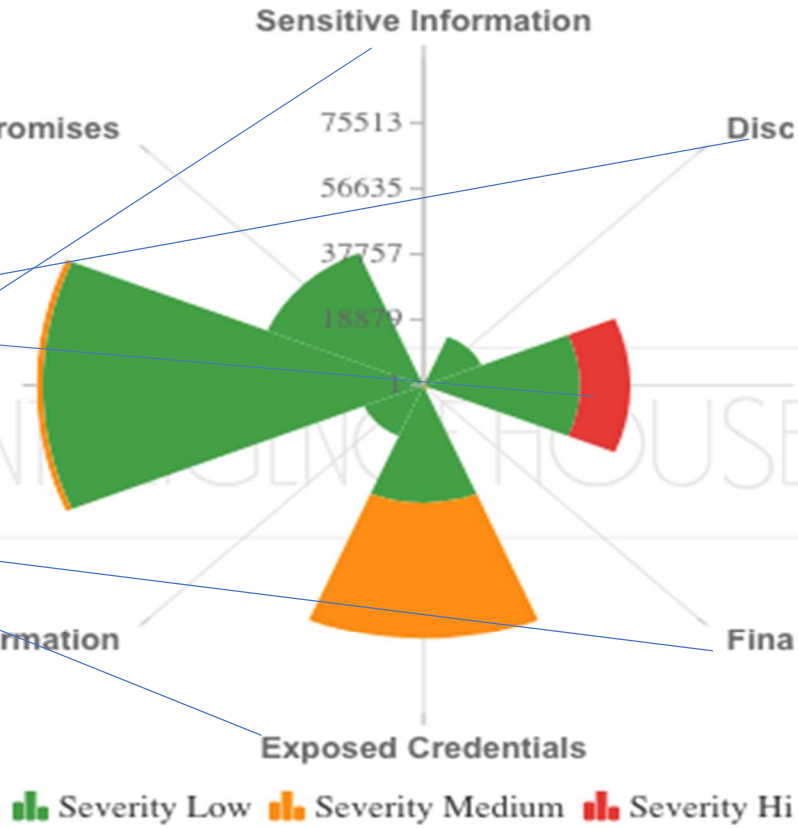




Exposure by Category

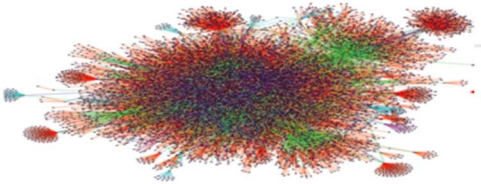
- Black Markets 16.76% (50465)
- Attacks & Compromises 13.71% (41269)
- Discussions 5.08% (15289)
- Exposed Credentials 24.25% (73016)
- Financial 0.36% (1075)
- Hacker Group Targeting 31.35% (94387)
- Personal Information 5.23% (15737)
- Sensitive Information 0.42% (1269)

Severity level per Exposure category

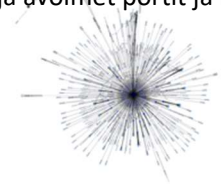


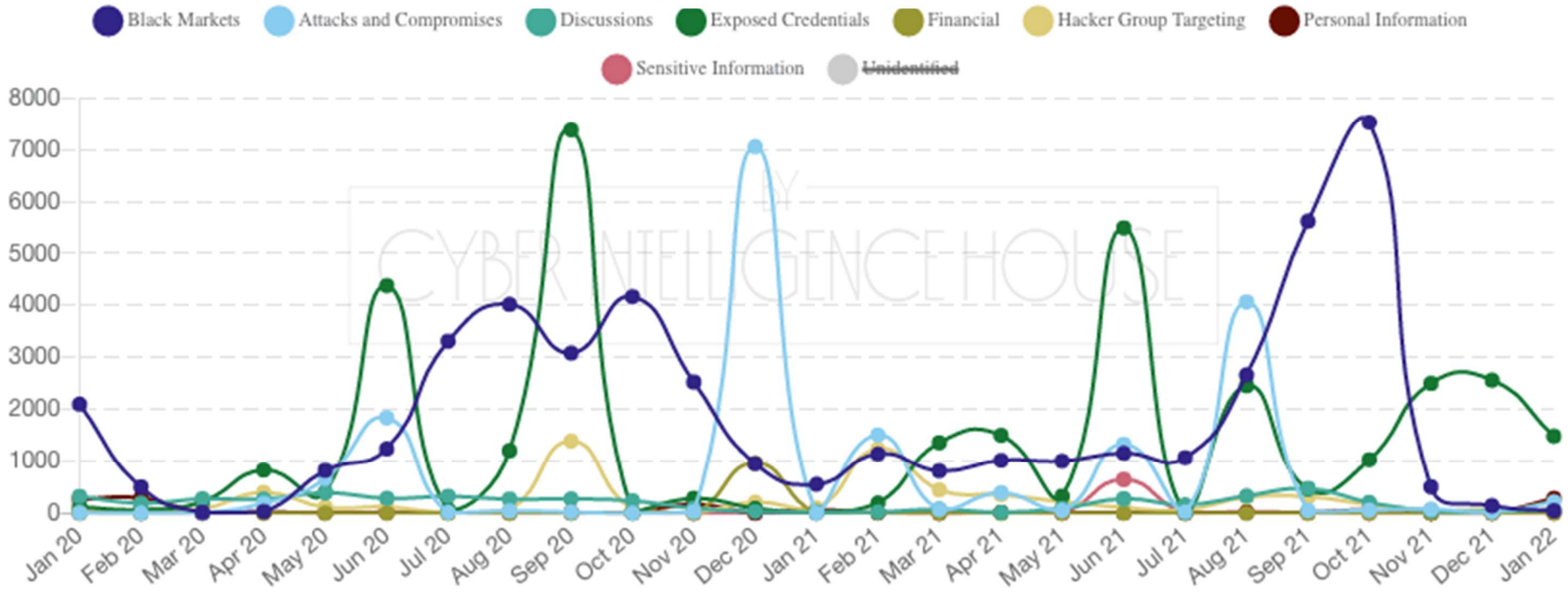
Exposure Trend

Hyökkäyspintala ja keskinäisriippuvuudet

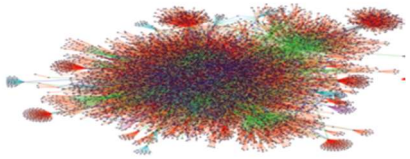


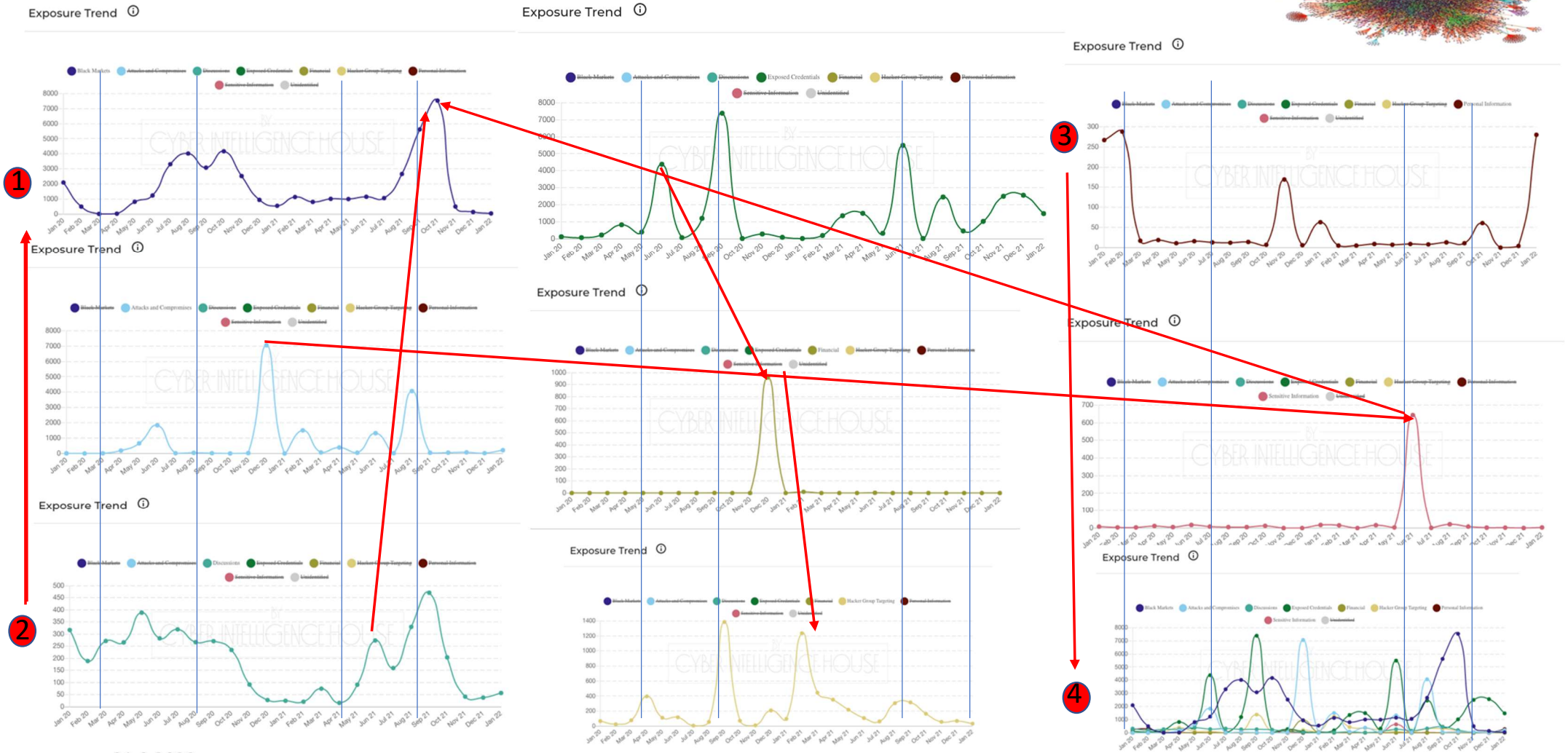
Domainit ja avoimet portit ja keskinäisriippuvuudet





Pimeä ja syväverkko (Dark ja Deep web) Hyökkäyspintalan muodostuminen.
Ihmiset ja päätelaitteet, riskit ja toimintatavat. Keskinäisriippuvuudet.

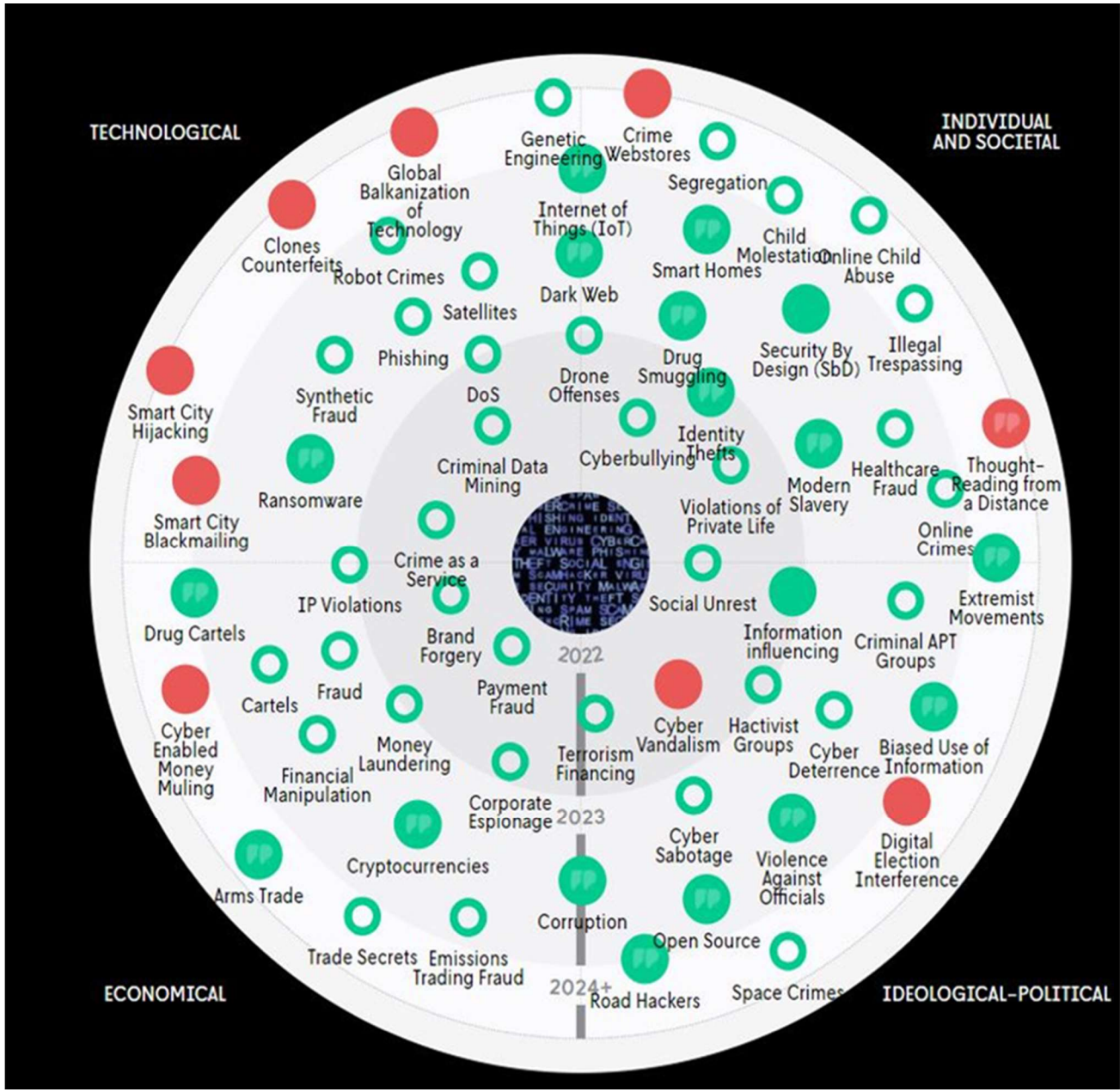


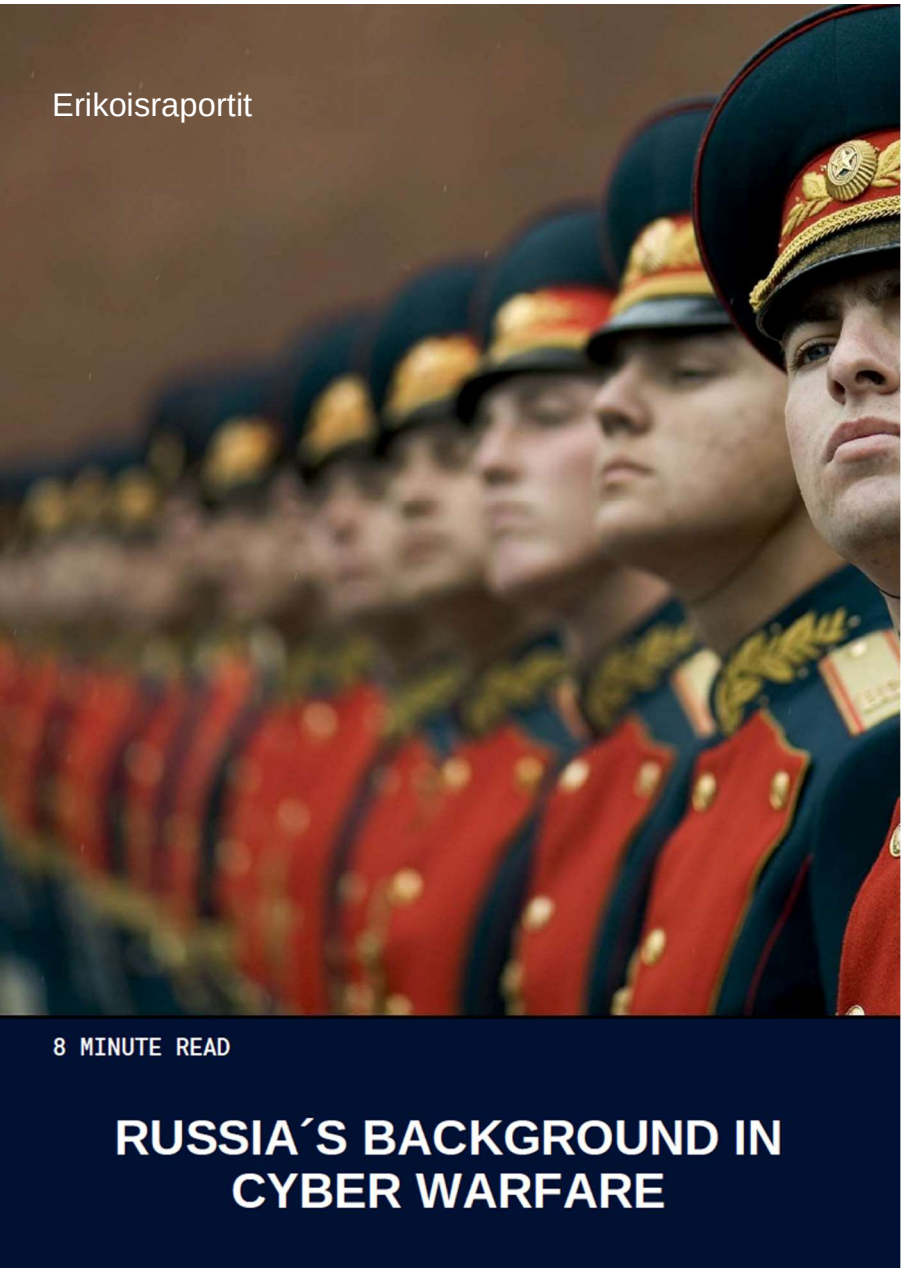


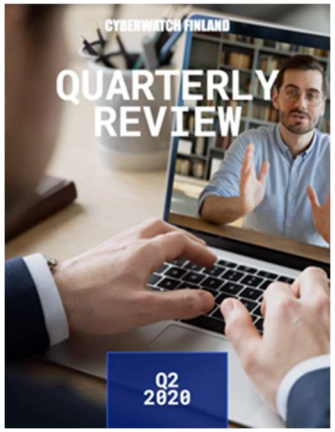
”SMART CYBERCRIME”

- Long definition: Smart cybercrime consists of criminal acts committed online in electronic communications networks or information systems by using advanced technologies and platforms to significantly increase the effectiveness, scale and agility of crime, at the same time, the complexity and the several dimensions of modus operandi make prevention, detection and investigation of smart cybercrime very challenging.

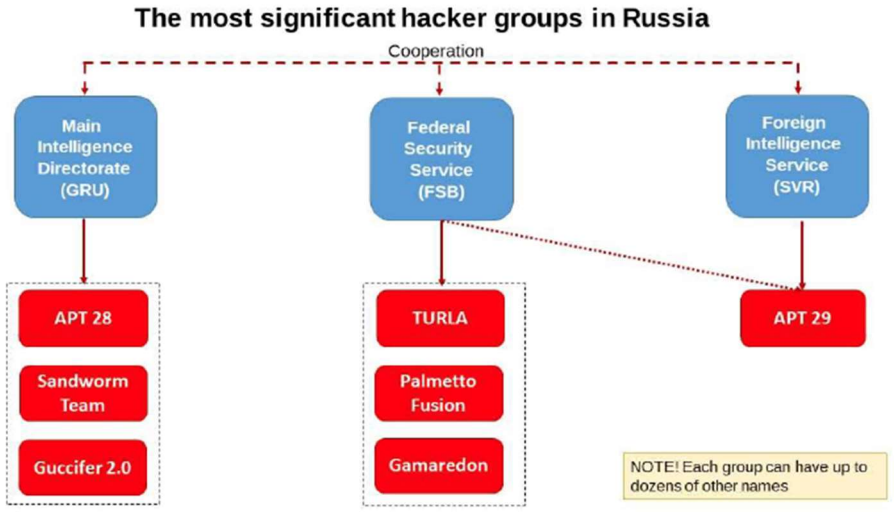
- Short definition: Cybercrimes have evolved to become more sophisticated and smarter. Advanced technologies and platforms have increased the efficiency and agility of crimes and also made prevention more challenging.





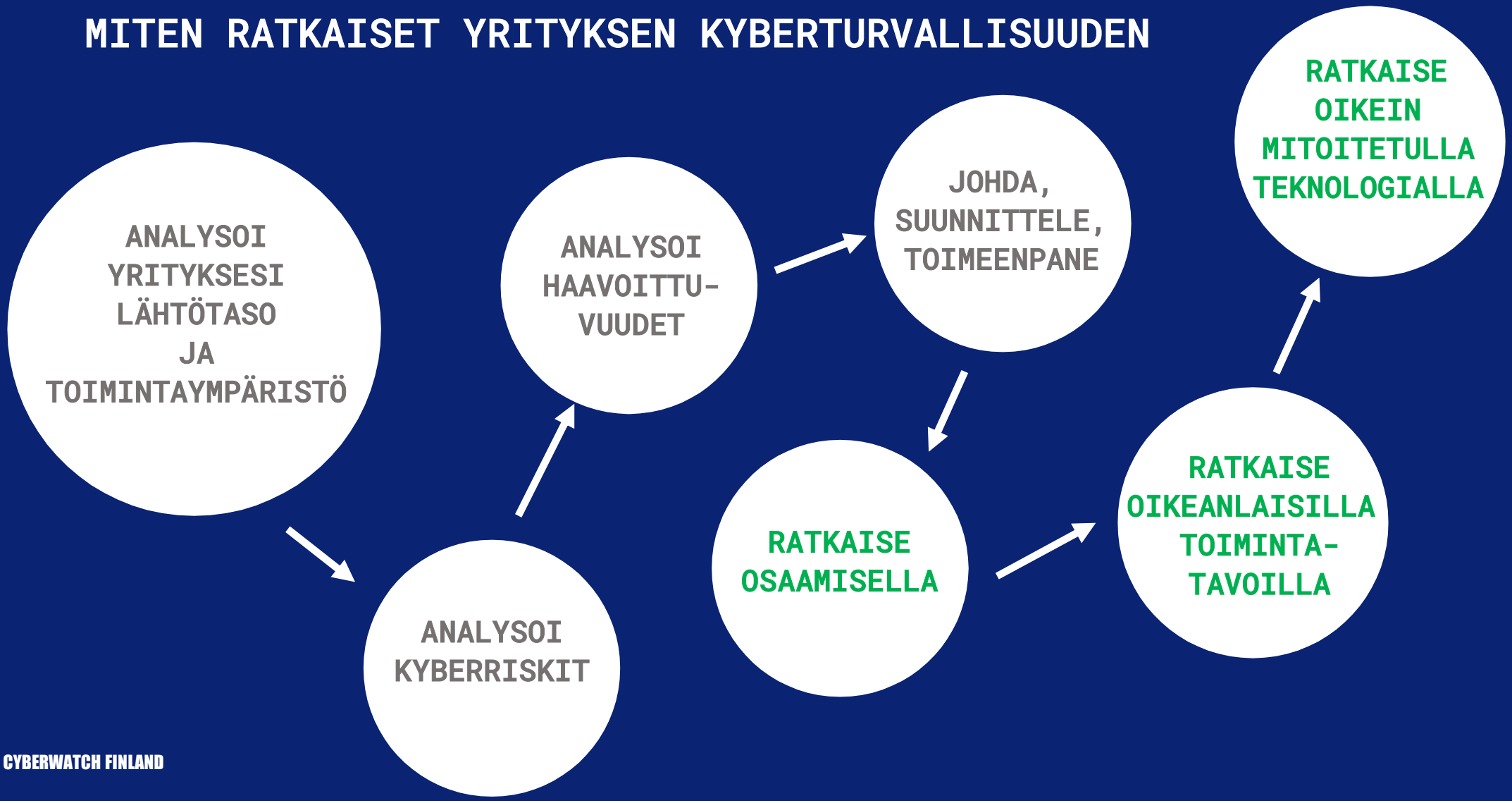


Tilannekuva muodostuu osaamisen kehittämisen kautta.
Katsaukset ja erikoisraportit



Sources: Cunningham, Conor: *A Russian Federation Information Warfare Primer*, Research report, University of Washington, 12.11.2020
Russian Cyber Units, Congressional Research Service, January 4, 2021

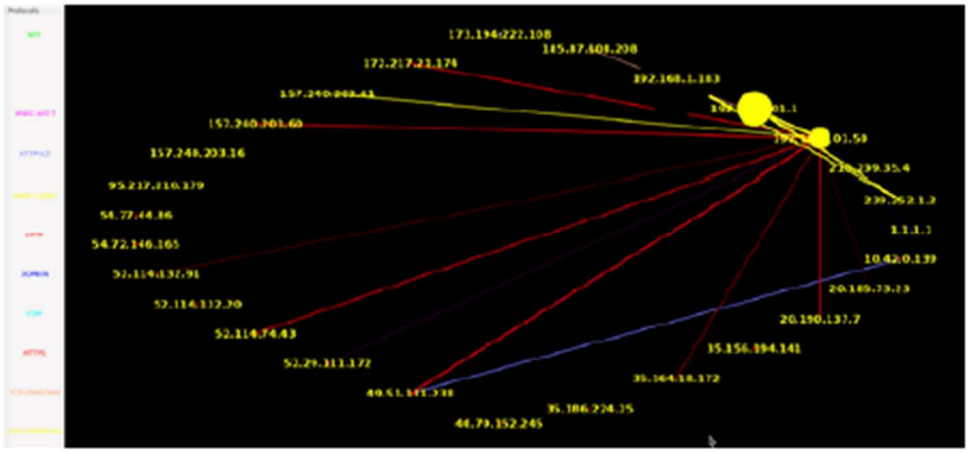
MITEN RATKAISET YRITYKSEN KYBERTURVALLISUUDEN



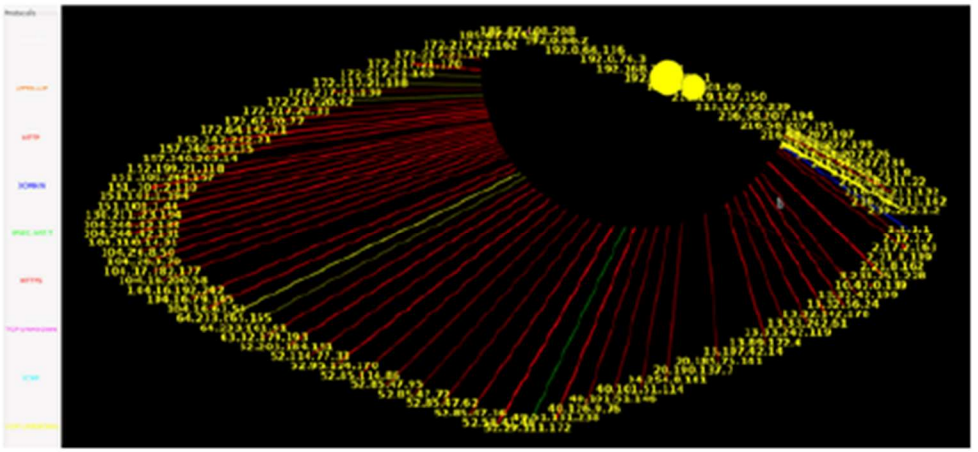
CYBERWATCH FINLAND

Koronavilkku on todettu turvalliseksi, mutta miten on ekosysteemin laita?

Koronavilkku on turvallinen mutta onko ympäristö missä sitä käytetään?



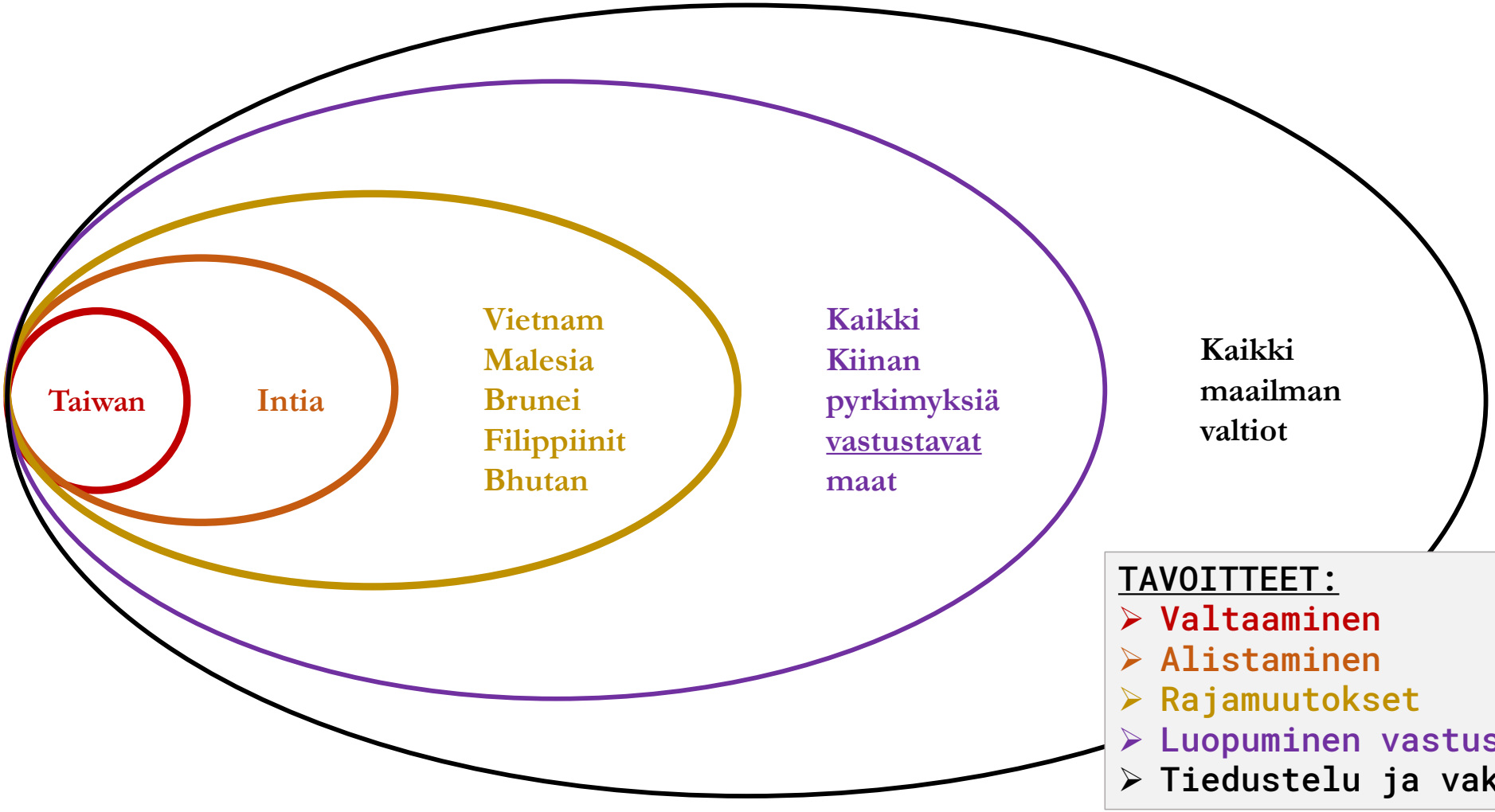
Korona vilkun käynnistys, puhelimen yhteydet eri IP osoitteisiin



Google avattu, Korona vilkku päällä, puhelimen yhteydet eri IP osoitteisiin

CYBERWATCH FINLAND

KIINAN HYBRIDISODANKÄYNNIN KOHTEET JA TAVOITTEET



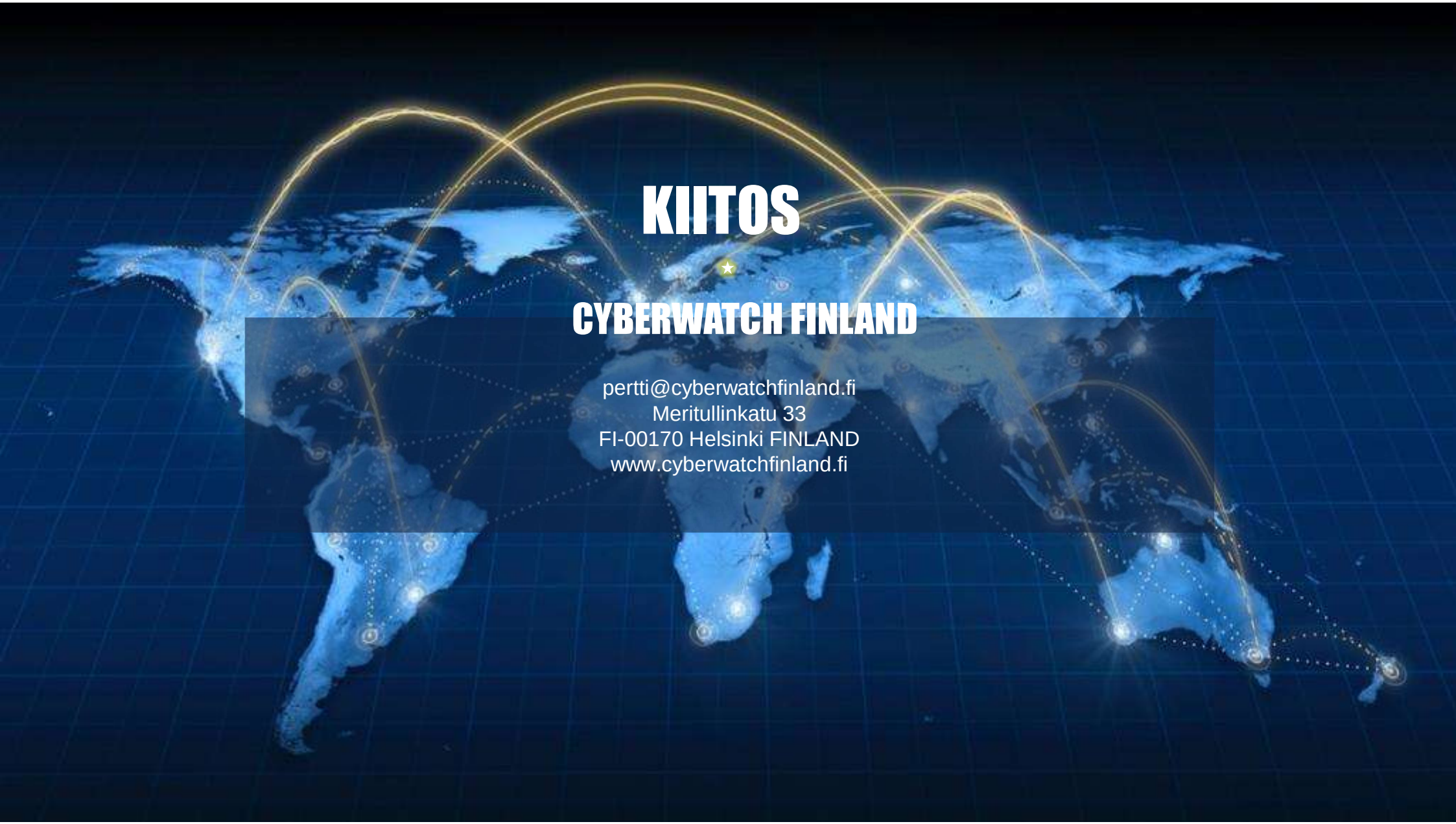
TAVOITTEET:

- Valtaaminen
- Alistaminen
- Rajamuutokset
- Luopuminen vastustamisest
- Tiedustelu ja vakoilu

Belarusian Cyber-Partisans
@cpartisans

🧵1/3🔥For the 1st time in human history a #hacktivist collective obtained passport info of the ALL country's citizens. Now we're offering you an opportunity to become a part of this history 😎. Get a unique digital version of #lukashenka passport as #NFT opensea.io/collection/cpa...


KYBERTURVALLISUUS SYNTYY PIENISTÄ TEOISTA JA KOKONAISUUDEN HALLINNASTA
CYBERWATCH FINLAND



KIITOS

CYBERWATCH FINLAND

pertti@cyberwatchfinland.fi
Meritullinkatu 33
FI-00170 Helsinki FINLAND
www.cyberwatchfinland.fi