Strategisen kyberturvallisuuden erikoisjulkaisu

Cyberwatch Finland

MAGAZINE 3/2024

KYBERSÄÄNTELYN HYÖKYAALTO

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

SISÄLLYS

3/2024

4

REGULAATION HYÖKYAALTO TULEE, OLEMMEKO VALMIITA

Vuoden vaihteessa voimaan tullut EU:n kyberturvallisuusdirektiivi NIS2 tullaan panemaan täytäntöön uudella kansallisella kyberturvallisuuslailla. Tavoitteena on saada laki voimaan lokakuussa 2024.

6

KYBERTURVALLISUUSSÄÄNTELYN AALLON HARJALLA

Kyberturvallisuuden ympärille rakentuu uutta sääntelyä nopeasti ja EU-vetoisesti. Syksyllä 2024 olemme ikään kuin hyökyaallon harjalla matkalla soveltamaan vääjäämättä etenevää uutta kyberturvasääntelyä.

12

EU:N SÄÄNTELYTSUNAMI ON TÄÄLLÄ – ONKO YRITYKSESI VALMIS?

Euroopan unionilla on kunnianhimoinen tavoite rakentaa parempaa digitaalista elämää eurooppalaisille. Tavoite ei kuitenkaan ole mikään ”Euroopasta tullut” ajatus, vaan meidän kaikkien demokraattisesti määritellyn yhteisen tahtotila.

16

AAVISTUKSISTA ENNUSTUKSIIN: IHMISEN JA KONEEN ÄLYKKYYKSIEN YHDISTÄMINEN SEKÄ TILANNEYMMÄRRYKSEN SAAVUTTAMISEEN KYBERINFORMAATIOSTA

Miten hybridi-informaation vaikutusta konfliktitilanteissa voidaan havaita, seurata ja torjua?

24

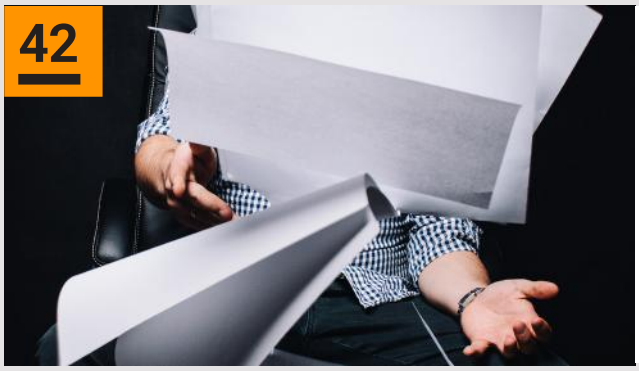
SANANVAPAUDEN PUOLUSTAMINEN VAPAALLA VALINNALLA - KOHTI KOKO YHTEISKUNNAN KATTAVIA TEKNOLOGIAVETOISIA, IHMISKESKEISIÄ PÄÄTELAITERATKAISUJA

Kansankiihottajien nousu demokratian kautta ei ole uusi ilmiö, kuten eivät myöskään heidän yrityksensä hyödyntää uusia viestintävälineitä propagandan levittämiseen, kansalaisten manipulointiin ja lopulta tyranniaan.

34

TAISTELEMMEKO VARJOSSA?

Sotia käydään usein muilla välineillä kuin sotilaallisella voimalla. Armeija voi kuitenkin tukea uhkaan vastaamista. Kovien keinojen lisäksi armeijat voivat tarjota poliittiselle johdolle arvokkaita neuvoja, menettelytapoja ja tekniikoita, joiden avulla hallitukset voivat torjua eksistentiaalisia uhkia.



42

CYBERWATCH FINLAND – MODERNIN DIGITAALISEN YHTEISKUNNAN HAASTEET JA RESILIENSSI

Cyberwatch Finland julkaisi elokuussa 2024 white paperin modernin digitaalisen yhteiskunnan haasteista ja resilienssistä. Tavoitteenamme on herättää keskustelua kyberturvallisuuden tilasta sekä jakaa keräämiämme oppeja viime vuosien ajalta.

46

CYBERWATCH FINLAND KUUKAUSIKATSAUS LOKAKUU 2024

56

UHKATIEDUSTELU-SEURANTA

Cyberwatch Magazine

Strategisen kyberturvallisuuden erikoisjulkaisu

JULKAISIJA
Cyberwatch Finland
Nuijamiestentie 5 C
04400 Helsinki
www.cyberwatchfinland.fi

TOIMITUS
Päätoimittaja
Aapo Cederberg
aapo@cyberwatchfinland.fi

Toimitussihteeri
Elina Tuomisto
elina@cyberwatchfinland.fi

ULKOASU JA TAITTO
Elina Tuomisto
elina@cyberwatchfinland.fi

KUVITUS
Gencraft
Pixabay
Shutterstock

ISSN 2490-0753 (print)
ISSN 2490-0761 (web)

PAINO
Scanseri Oy, Helsinki

REGULAATION HYÖKYAALTO TULEE, OLEMMEKO VALMIITA

// Aapo Cederberg

Tällä hetkellä geopoliittinen toimintaympäristö on erittäin epävakaa, johon vaikuttaa erityisesti Venäjän Ukrainaa vastaan aloittama hyökkäyssota. Venäjä katsoo käyvänsä kineettistä (perinteistä) sotaa Ukrainassa ja hybridisotaa länsimaista sivilisaatiota vastaan. Tämä on muuttanut turvallisuusympäristöämme pysyvästi. Kriittinen infrastruktuuri on ollut kineettisten ja ei-kineettisten iskujen pääkohde. Kybersodankäynti Ukrainassa on ollut vaikutuksiltaan odotettua vähäisempää. Venäjä näyttääkin käyttävän Ukrainassa mieluummin perinteistä sotavoimaa, jolla on suurempi tuho- ja pelotevaikutus, kuin älykkäitä kyberoperaatioita, joita niiden paljastumisen jälkeen on vaikea käyttää uudestaan.

Näyttääkin siltä, että älykkäimmät kyberoperaatiot säästetään hybridivaikuttamisen välineiksi länsimaita vastaan. Näin pystytään operoimaan perinteisen sodan kynnyksen alapuolella ja saadaan aikaan informaatio-psykologisia pelotevaikutuksia. Kognitiivinen sodankäynti on tullut vahvasti osaksi epäsymmetristä sodankäyntiä. Kansalaisten henkistä kriisinkestävyyttä pyritään horjuttamaan pitkäkestoisella hybridioperoinnilla. Sodalle ei ole loppua näkyvissä, joten yhteiskunnan kriittisten toimintojen ja palveluiden turvaamiseen on panostettava jatkuvasti enemmän. Varautumistoimenpiteiden tulee kattaa koko yhteiskunta ja kaikki toimijat.

Vuoden vaihteessa voimaan tullut EU:n kyberturvallisuusdirektiivi NIS2 tullaan panemaan täytäntöön uudella kansallisella kyberturvallisuuslailla. Tavoitteena on saada laki voimaan lokakuussa 2024. Siinä säädetään, miten käytännössä toteutetaan direktiivin velvoitteet yritysten osalta. Julkisen sektorin osalta velvoitteista säädettään päivittämällä tiedonhallinta lakia. Muutokset ovat merkittäviä. Kriittiset toimijat joutuvat päivittämään kyberturvallisuuden järjestelynsä, ottaen huomioon NIS2-direktiivin ja kansallisen lainsäädännön vaatimukset. Uudet velvoitteet kattavat kyberturvallisuuden riskienhallinnan, johdon vastuun, poikkeamien raportoinnin ja ilmoittautumisen toimivaltaisen viranomaisen ylläpitämään toimijaluetteloon vuoden 2024 loppuun mennessä. Kyberturvallisuus tulee siten pakolliseksi erityisesti keskeisille toimijoille ja velvoitteiden laiminlyöminen voi johtaa sakkomaksuihin. Jokaisen yrityksen tulee itse määritellä mihin kategoriaan kuuluu ja tehtävä tarvittavat ilmoitukset. Tämä alleviivaa johdon tarvetta perehtyä kyberturvallisuuteen ja voimaan tulevan uuden lainsäädännön vaatimuksiin.

Mielestäni tätä prosessia kannattaa tarkastella positiivisena kehityksenä, kyberuhka jatkaa kasvamistaan ja meidän kaikkien on joka tapauksessa tehtävä kehittämistoimenpiteitä. Uudet juridiset velvoitteet kohdistuvat aivan oikeisiin asioihin, joiden tulee olla kunnossa, jotta voimme paremmin vastat kybermaailman tuleviin haasteisiin.

Euroopan kriittistä infrastruktuurin suojaamista koskeva ECI-direktiivi korvataan uudella CER- direktiivillä. (Critical Entitied Resilience), jota kutsutaan myös resilienssidirektiiviksi. CER perustuu EU:n turvallisuusstrategiaan, jossa linjattiin mm. että ”jokapäiväisessä elämässämme käytettävien elintärkeiden infrastruktuurien tulee olla turvattuja ja kestäviä”. Direktiivin soveltamisala kattaa yksitoista sektoria: liikenne-, energia-, pankki-, finanssi-, terveys-, vesihuolto- ja jätevesihuoltosektorit, ruoka sekä digitaalisen infrastruktuurin, julkishallinnon ja avaruuden.

Tämän kokonaisuuden tulee kulkea kyberturvallisuusdirektiivin kanssa käsikädessä, erityisesti siksi, että kriittinen infrastruktuuri on keskeisin kyberhyökkäysten kohde. Finanssialalla riskienhallinnassa tulee noudattaa ns. DORA-asetusta, joka on NIS2-sääntelyä huomattavasti yksityiskohtaisempi.

Kaikella tällä regulaatiolla pyritään yhtenäistämään ja parantamaan kyberturvallisuuden tasoa kokoa EU:n alueella. Tämä on erityisen tärkeää kilpailukyvyn vahvistamisen ja digitaalisen itsenäisyyden näkökulmasta. Yritysten hallitusten ja operatiivisen johdon tuleekin ymmärtää, että emme vain varaudu uhkiin ja riskeihin vaan vahdistamme omaa kilpailukykyämme ja luomme uusia liiketoimintamahdollisuuksia. NIS2-sääntelyn mukaan toimiva johto on vastuussa kyberturvallisuuden riskienhallinnan järjestämisestä ja sen toteuttamisen valvonnasta. Kyberturvallisuuden riskienhallinnan toimintamallin tulee olla toimivan johdon hyväksymä ja lisäksi johdolla tulee olla ajantasainen kuva yrityksen kyberturvallisuuden tilasta.

Julkaisimme elokuussa white paperin modernin digitaalisen yhteiskunnan haasteista ja resilienssistä. Tavoitteenamme on herättää keskustelua kyberturvallisuuden tilasta sekä jakaa Ukrainan sodasta tekemiämme johtopäätöksiä. Suomessakin yksityisen sektorin rooli aloitteiden tekijänä voisi olla vahvempi ja ajatuspajatoimintaa voitaisiin lisätä. Mielestämme white paper itsessään on sopiva formaatti uusien ajatusten esittämiselle. Tarkoituksenamme ei ole arvostella ketään vaan ajatella ääneen. Saamamme palaute on ollut erittäin positiivista ja kannustavaa. White paper on vapaasti luettavissa kotisivuillamme. Toivottavasti keskustelu jatkuu. ■

AAPO CEDERBERG

- Toimitusjohtaja ja perustaja
- **Cyberwatch Finland**

KYBERTURVALLISUUSSÄÄNTELYN AALLON HARJALLA

// Jukka Lång, Joona Linner ja Johanna Tuohino

Kyberturvallisuuden ympärille rakentuu uutta sääntelyä nopeasti ja EU-vetoisesti. Syksyllä 2024 olemme ikään kuin hyökyaallon harjalla matkalla soveltamaan vääjäämättä etenevää uutta kyberturvasääntelyä. Tähän sääntelykokonaisuuteen sisältyy säädöksiä, joilla pyritään luomaan kyberturvallisuuden hallinnalle EU:n laajuisia kehyksiä ja parantamaan muun muassa EU:n sisämarkkinoilla tarjottavien tuotteiden sekä kriittisten infrastruktuurien ja toimijoiden turvallisuutta.

NIS2 ((EU) 2022/2555) ja CER ((EU) 2022/2557) -direktiivit ovat tänä syksynä erityisen ajankohtaisia ja niihin tartutaan jäljempänä. Sitä ennen katsotaan hetkeksi taaksepäin olemassa olevaan kyberturvasääntelyyn.

EU:N TIETOSUOJA-ASETUS VELVOITTAA HENKILÖTIETOJEN KÄSITTELYN TURVALLISUUTEEN

Yksi olemassa olevan kyberturvasääntelyn keskeisimmistä kokonaisuuksista sisältyy EU:n yleiseen tietosuoja-asetukseen (EU) 2016/679 ("GDPR"). GDPR:n elementit muodostavat EU:n sisämarkkinoilla kaikkiin yrityksiin ja muihin organisaatioihin soveltuvan kyberturvallisuuden lähtötason henkilötietojen käsittelylle. GDPR asettaa tietoturvallisuutta koskevia velvoitteita myös niille organisaatioille, jotka eivät kuulu toimialakohtaisen kyberturvallisuussääntelyn soveltamisalaan. Tietoturva (eheys ja luottamuksellisuus) on yksi GDPR:n mukaisista tietosuojaperiaatteista eli yksi keskeisistä henkilötietojen käsittelemisen periaatteista. Muita GDPR:n kyberturvallisuusliitännäisiä elementtejä ovat esimerkiksi tietosuojan vaikutustenarviointia (DPIA) sekä tietoturvaloukkausten raportointia ja niistä rekisteröidyille ilmoittamista koskevat säännökset. GDPR:n mukainen velvollisuus solmia tietojenkäsittelysopimus rekisterinpitäjän ja sen käyttämän henkilötietojen käsittelijänä toimivan tahon välillä sekä siihen liitännäinen kansainvälisiä tiedonsiirtoja koskeva sääntely ovat osa toimitusketjujen turvallisuuden varmistamista.

Nämä edellä mainitut kokonaisuudet ovat merkittäviä uuden kyberturvasääntelyn rinnalla, sillä tietosuoja- ja kyberturvasääntely vaatimuksineen johtaa useissa tapauksissa päällekkäisiin tai rinnakkaisiin vaatimuksiin esimerkiksi poikkeamien hallinnassa ja toimitusketjujen turvallisuuden varmistamisessa. Joissain tapauksissa tietosuojaa ja tietoturvaa joudutaan myös punnitsemaan rinnakkain.

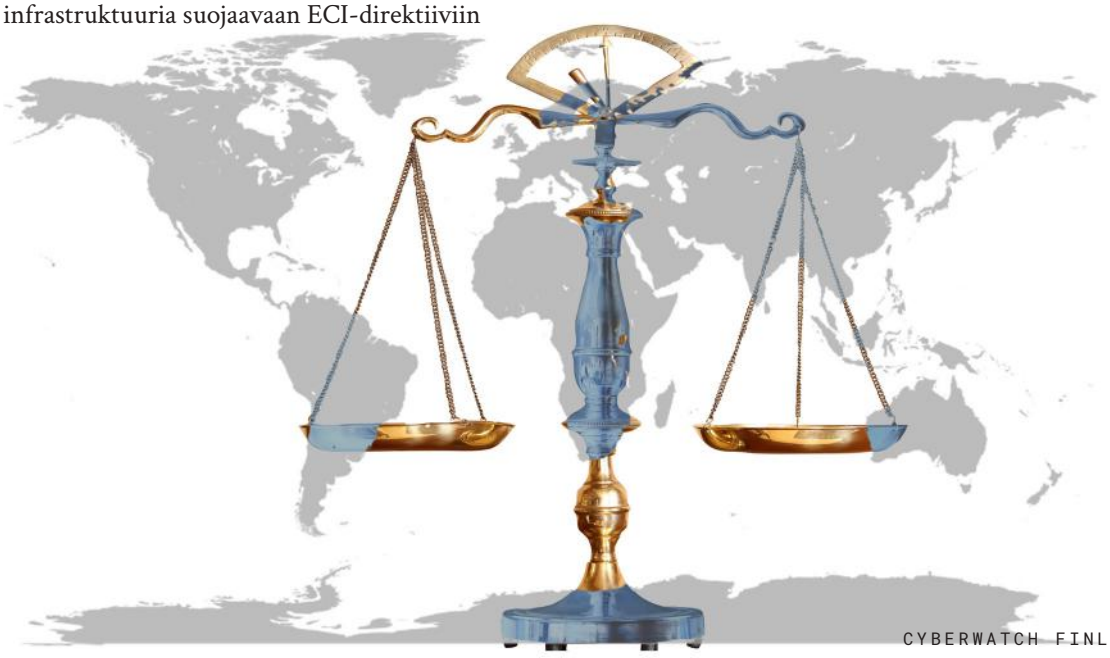
KYBERTURVALLISUUSASETUS TOISEN SUKUPOLVEN KYBERTURVASÄÄNTELYN PERUSTANA

Niin sanottu ensimmäisen sukupolven eurooppalainen kyberturvasääntely viittaa verkko- ja tietoturvaa koskevaan NIS-direktiiviin (2016/1148) sekä Euroopan kriittistä infrastruktuuria suojaavaan ECI-direktiiviin (2008/114EC). NIS-direktiivin korvaava NIS2-direktiivi on soveltamisalaltaan edeltäjäänsä laajempi. Jäljempänä käsitelty CER-direktiivi puolestaan korvaa ECI-direktiivin.

Toisen sukupolven kyberturvallisuussääntelyn perustan muodostaa EU:n kyberturvallisuusasetus ((EU) 2019/881). Kyberturvallisuusasetuksella perustettiin Euroopan kyberturvallisuusvirasto ENISA sekä kehys eurooppalaiselle kyberturvallisuuden sertifioinnille. EU-lainsäätäjien tulevaisuuden tavoitteena on, että NIS2-sääntelyn soveltamisalaan kuuluvat toimijat soveltaisivat relevantteja kyberturvallisuusasetuksen sertifiointijärjestelmän mukaisia standardeja. Toistaiseksi tämän sertifiointijärjestelmän EU-tasoinen käyttöönottaminen on vielä kesken. Tällä hetkellä sertifiointijärjestelmän alla on muodostettu standardit koskien älykortteja, mikrosiruja ja digitaalisia lompakkoja.

NIS2-DIREKTIIVI LAAJENTAA KYBERTURVALLISUUDEN RISKIENHALLINTAVELVOITTEITA KRIITTISILLÄ TOIMIALOILLA

23. toukokuuta 2024 Suomi otti merkittävän askeleen kohti kyberturvallisuuslainsäädännön vahvistamista, kun hallitus antoi eduskunnalle esityksen (HE 57/2024 vp) NIS2-direktiivin täytäntöönpanemiseksi uudella kyberturvallisuuslailla ja julkisten hallinnon tiedonhallinnasta annetun lain muutoksilla. Tämän NIS2-sääntelyn tavoitteena on tehostaa kyberturvallisuutta kriittisillä toimialoilla ja siirtää sääntelyn painopistettä kyberturvallisuuden riskienhallintaan ja poikkeamien raportointiin. Sääntelyn on määrä tulla sovellettavaksi 18.10.2024 lähtien.



NIS2-SÄÄNTELYN LÄHTÖKOHDAT

NIS2-direktiivi ja sen kansallinen täytäntöönpano laajentavat merkittävästi kyberturvallisuusvaatimusten soveltamisalaa, kattaen keskisuuret ja suuret toimijat kriittisillä sektoreilla. Näihin sektoreihin kuuluvat muun muassa energia, liikenne, terveydenhuolto, digitaalinen infrastruktuuri, sekä kokonaan uudet sektorit, kuten julkishallinto, elintarviketuotanto, jätehuolto ja tietyt teollisuudenalat, joita NIS2-direktiivin edeltäjä (NIS-direktiivi) ei kattanut. Huomionarvoista on, että uudet vaatimukset koskevat tiettyjä toimijoita koosta riippumatta, kuten julkisten sähköisten viestintäverkkojen ja -palvelujen tarjoajia. Lisäksi tietyt soveltamisalaan kuuluvat toimijat ovat keskeisiä toimijoita, ja siten kuuluvat tiukemman valvonnan ja ankarampien sanktioiden piiriin.

NIS2-sääntelyssä eriteltyjen kriittisten toimialojen toimijoiden osalta sääntely soveltuu toimijaan kokonaisuudessaan (oikeushenkilökohtaisuus). Pääsäännön mukaan NIS2-sääntelyn piiriin kuuluvalla toimialalla toimivan toimijan (oikeushenkilön) sijoittautumismaa määrittää sen, minkä jäsenvaltion kansallinen sääntely soveltuu. ICT-palveluiden hallinta ja digitaalinen infrastruktuuri -toimialojen osalta NIS2-sääntelyn alueellinen sovellettavuus määräytyy poikkeuksellisesti toimijan päätoimipaikan mukaan Euroopan tasolla.

NIS2-sääntelyn alaan kuuluvat toimijat joutuvat uudelleenarvioimaan ja päivittämään kyberturvallisuuskäytäntöjään suhteessa uusiin kyberturvallisuusvaatimuksiin. Uudet vaatimukset kattavat kyberturvallisuuden riskienhallinnan, johdon vastuun, poikkeamien raportoinnin ja ilmoittautumisen toimivaltaisen viranomaisen ylläpitämään toimijaluetteloon vuoden 2024 loppuun mennessä.

Uudet vaatimukset tulevat myös todennäköisesti muuttamaan ICT-järjestelmien kyberturvallisuuteen liittyviä sopimuksia ja sopimusehtoja laajemmin kuin vain NIS2-sääntelyn soveltamisalaan kuuluvien sektorien sisällä.

KYBERTURVALLISUUDEN RISKIENHALLINTA

Toimijoiden on otettava käyttöön kattava kyberturvallisuuden riskienhallinnan toimintamalli. Toimintamallin on sisällettävä tekniset, operatiiviset ja organisatoriset toimenpiteet, jotka on suunniteltu suojaamaan toimijan viestintäverkkoja ja tietojärjestelmiä sekä lieventämään poikkeamien haitallisia vaikutuksia. Riskienhallinnan toimintamallin keskeiset elementit ovat:

- **Riskiarviot ja analyysit:** Toimintamallin on oltava riskeihin perustuva ja kaikki uhkat huomioiva , jotta toimijat voivat ennakoivasti tunnistaa ja käsitellä mahdollisia uhkia eri lähteistä.
- **Dokumentointi:** Toimijoiden on määriteltävä, kuvattava ja dokumentoitava riskienhallinnan tavoitteet, prosessit ja vastuut. Dokumentoitua riskienhallinnan toimintamallia on pidettävä ajan tasalla. Toimintamallin on oltava toimijan ylimmän johdon hyväksymä.
- **Hallintatoimia koskevat vähimmäisvelvoitteet:** Riskienhallintamallin on sisällettävä vähintään lainsäädännössä luetellut vähimmäistoimenpiteet ja -kokonaisuudet.

KYBERRISKIENHALLINNAN HALLINTATOIMIA KOSKEVAT VÄHIMMÄISVELVOITTEET

Kyberturvallisuuden riskienhallinnan toimintamallissa on huomioitava NIS2-sääntelyn edellyttämät vähimmäisvelvoitteet. Seuraavassa on kuvattu teemat, jotka tulisi vähintään huomioida tarvittavia hallintatoimia arvioitaessa ja implementoitaessa:

- Verkkojen ja järjestelmien turvallisuutta koskevat toimintaperiaatteet ja riskienhallintapolitiikka;
- Politiikat ja prosessit toimintamallin mukaisesti määriteltyjen hallintatoimenpiteiden vaikuttavuuden arvioimiseksi;
- Verkkojen ja järjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä haavoittuvuuksien tunnistaminen ja käsittely:
    - (i) Toimittajien valintaa koskevien kriteerien määrittäminen sekä liitännäiset riskiarviot, (ii) turvallisen kehittämisen elinkaari, (iii) konfiguraatioiden ja muutosten hallinta, (iv) korjaukset ja ylläpito, (v) turvallisuuden testaaminen, (vi) päivitysten hallinta, (vii) verkkoturvallisuus ja segmentointi, (viii) suojaus haitallisilta ja luvattomilta ohjelmistoilta sekä (ix) haavoittuvuuksien käsittely ja julkistaminen;
- Toimitusketjujen turvallisuus, ml. turvallisuutta koskevat politiikat, sopimuskäytännöt sekä luettelot toimittajista ja palveluntarjoajista;
- Omaisuudenhallinta, ml. omaisuuden luokittelu ja käsittely, päätelaitteita ja tallennusvälineitä koskevat politiikat, omaisuusluettelot (inventointi) sekä omaisuuden palauttaminen ja tuhoaminen myös henkilöstöturvallisuuden osa-alueena;
- Henkilöstöturvallisuus (ml. toimittajien henkilöstö), kuten taustojen selvittäminen, sopimusehdot ja kurinpitomenettelyt sekä irtisanomista ja tehtävien vaihtamista koskevat menettelyt;
- Pääsynhallinta ja todentamisen menettelyt, ml. pääsynhallintapolitiikat sekä tarvittaessa monivaiheinen todentaminen (MFA) ja mahdolliset jatkuvan todentamisen ratkaisut;
- Salausmenetelmien ja kryptografian käyttämistä koskevat toimintaperiaatteet ja menettelyt, ml. liitännäiset riskiarviot, tietojen luokittelut ja eri luokille sovellettavat salaustasot;
- Poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi:
    - (i) poikkeamien käsittelyä koskeva politiikka, (ii) valvonta ja lokit sekä muut toiminnot, joista vaarantumisindikaattoreita on kerättävissä, (iii) poikkeamien arviointi ja luokittelu, (iv) poikkeamiin vastaaminen ja (v) juurisyiden arvioimiseen sekä muut jälkitoimet, joilla pienennetään riskiä vastaavan poikkeaman tapahtumiselle vastaisuudessa;
- Varmuuskopiointi sekä toiminnan jatkuvuuden- ja kriisinhallinta, ml. liitännäiset suunnitelmat ja tarvittaessa varaviestintäjärjestelmien käyttöönotto;
- Perustason tietoturvakäytännöt ja tietoisuus, ml. turvallisuusharjoitukset ja perustason kyberhygieniakäytännöt, perustason tietoisuuden lisääminen ja lisäkoulutukset/-harjoitukset tehtäväkohtaisten riskiarvioiden perusteella (räätälöidyt syventävät koulutukset);
- Toimet verkkojen ja järjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi, ml. varavirtalähteet, turva-alueiden määrittely ja fyysinen kulunvalvonta sekä suojautuminen fyysisiltä ja ympäristöuhilta.

JOHDON VASTUU

Ehdotetun NIS2-sääntelyn mukaan toimijan johto on vastuussa kyberturvallisuuden riskienhallinnan järjestämisestä ja sen toteuttamisen valvonnasta. Kyberturvallisuuden riskienhallinnan toimintamallin tulee olla toimijan johdon hyväksymä ja lisäksi johdolla tulee olla ajantasainen kuvaa toimijan kyberturvallisuuden tilasta.

Suomessa toimijan johdolla tarkoitetaan toimijan hallituksen ja hallintoneuvoston jäseniä (sekä tilanteen mukaan näiden varajäseniä) ja toimitusjohtajaa. Lisäksi toimijan johdolla voidaan tarkoittaa myös muita henkilöitä, jotka tosiasiallisesti johtavat toimijan toimintaa.

Määritelty johdon vastuu korostaa tarvetta ja vaatimusta johdon riittävälle kyberturvallisuuden riskienhallinnan tuntemukselle sekä tarpeelle uudelleen tarkastella sisäisiä päätöksenteko- ja raportointiprosesseja, jotta johto voi tosiasiallisesti ottaa NIS2:sen mukaisen vastuun kyberturvallisuuden hallintaan liittyen.

TOIMITUSKETJUJEN TURVALLISUUS

Uusien kyberturvallisuuden riskienhallintavaatimusten myötä erityisesti toimitusketjut on arvioitava uudelleen. Toimijoiden on otettava huomioon tuotteiden ja palveluiden kokonaislaatu, integroitu riskienhallinta sekä välittömien toimittajien kyberturvallisuuskäytännöt. Toimijoiden vastuulla on varmistaa, että valitut ja käytössä olevat tuotteet ja palvelut täyttävät toimijan riskienhallinnan toimintamallin mukaiset kyberturvallisuusvaatimukset. Käytännössä tämä tarkoittaa muun muassa sopimusehtojen tarkistamista toimittajien kanssa.

On syytä huomata, että toimitusketjujen turvallisuutta koskevat vaatimukset kohdistuvat sääntelyn alaan kuuluvaan toimijaan, mutta velvoitteet eivät suoraan kohdistu toimijan järjestelmä- tai laitetoimittajiin. Toimittajat voivat olla itsekin sääntelyn piirissä, mutta tällöin ne tarkastelevat riskienhallintaa oman toimintansa näkökulmasta.

POIKKEAMIEN RAPORTOINTI

Poikkeamien raportoiminen on uuden kyberturvallisuussääntelyn keskiössä ja raportoinnin laiminlyönti voi johtaa hallinnollisen sanktion määräämiseen.

Toimijoiden on raportoitava merkittävistä poikkeamista toimivaltaiselle valvontaviranomaiselle noudattaen seuraavaa raportointiprosessia:

1. Ensi-ilmoitus 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta.
2. Jatkoilmoitus 72 tunnin kuluessa merkittävän poikkeaman havaitsemisesta.
3. Loppuraportti kuukauden kuluessa jatkoilmoituksesta tai käsittelyn päättymisestä.

Kyseessä on **merkittävä poikkeama**, jos se aiheuttaa tai voi aiheuttaa jonkin seuraavista:

- → vakava palveluiden **toimintahäiriö**;
- → huomattava **taloudellinen tappio** toimijalle; tai
- → muille luonnollisille tai oikeushenkilöille huomattava **aineellinen tai aineeton vahinko.**

Merkittävän poikkeaman määrittelemiseen liittyvät yksityiskohtaiset ohjeet ja tulkinnat odotetaan selkiytyvän Euroopan komission täytäntöönpanosäänteln ja valvontaviranomaisten ohjeistusten myötä lähitulevaisuudessa.

VALVONTAVIRANOMAISET JA TÄYTÄNTÖÖNPANO

Suomessa NIS2-sääntelyn valvonta hajautetaan. Sektoreiden valvontaviranomaiset valvovat lain noudattamista omilla vastuualueillaan. Esimerkiksi Liikenne- ja viestintävirasto (Traficom) valvoo digitaalisen infrastruktuurin toimijoita, kun taas Energiavirasto valvoo sähköalan toimijoita. Useilla sektoreilla toimiva toimija voi olla usean valvontaviranomaisen alainen.

Traficomissa toimiva Kyberturvallisuuskeskus toimii yhteyspisteenä ja koordinoi valvontaviranomaisten toimintaa. Lisäksi Traficomiin perustetaan kansallinen CSIRT-yksikkö, joka tulee olemaan keskeisessä asemassa kyberuhkien ja poikkeamien seurannassa, analysoinnissa ja avustamisessa.

NIS2-sääntely antaa valvontaviranomaisille laajat valtuudet, mukaan lukien oikeuden saada tietoja, tarkastusoikeudet sekä mahdollisuuden antaa määräyksiä ja varoituksia.

JUKKA LÅNG

- Partner, Head of Data Protection & Cyber Security, asianajaja, CIPP/E
- Jukka Lång vetää Dittmar & Indreniuksen Data Protection & Cyber Security -osaamisaluetta. Jukka tunnetaan Suomen johtavana tietosuoja-asiantuntijana ja hän yksi Suomen harvoista kyberturvallisuussääntelyyn erikoistuneista osakastason asianajajista.
- **Dittmar & Indrenius**

CER- JA DORA-SÄÄNTELYN SUHDE NIS2-SÄÄNTELYYN

Siinä missä NIS2-sääntelyn puitteissa suojaudutaan kaikilta viestintäverkkoihin ja tietojärjestelmiin ja niihin sisältyviin tietovarantoihin kohdistuvilta uhilta, CER-direktiivin mukaiset riskienhallintavelvoitteet ulottuvat uhkiin, jotka voivat kohdistua TVT-järjestelmän lisäksi mihin tahansa muuhun toimintoon, jota tarvitaan kriittiseksi määritellyn palvelun tarjoamiseksi. Lisäksi CER-direktiivin alaan kuuluvien kriittisten toimijoiden ei tarvitse itse arvioida sitä kuuluvatko ne CER-direktiiviä implementoivan kansallisen lainsäädännön alaan. Lain soveltamisalaan kuuluvat toimijat tullaan nimeämään erikseen kriittisiksi toimijoiksi.

Kun toimija on nimetty CER-direktiivin nojalla kriittiseksi toimijaksi, kyseinen toimija on myös automaattisesti koosta riippumatta NIS2-sääntelyssä tarkoitettu keskeinen toimija. CER-direktiivin täytäntöönpanevan kansallisen lain olisi tarkoitus tulla sovellettavaksi viimeistään 18.10.2024, mutta lainvalmistelussa on aiheutunut viiveitä tämän artikkelin kirjoittamisen hetken tietojen mukaan.

DORA on finanssiyhteisöihin soveltuva kyberturvallisuuden riskienhallintaa koskeva EU-asetus ((EU) 2022/2554), joka on suoraan sovellettava kaikissa jäsenvaltiossa. DORA on huomattavasti NIS2-sääntelyä yksityiskohtaisempi ja finanssiyhteisöt soveltavat NIS2-sääntelyn sijaan DORA-asetusta. Lisäksi DORA:n nojalla on annettu huomattava määrä tarkentavaa sääntelyä. DORA-asetus on jo voimassa, mutta sitä aletaan soveltaa 17. päivänä tammikuuta 2025.

KATSE KOHTI TULEVAA

NIS2, CER ja DORA ovat merkittäviä säädöksiä uuden kyberturvallisuussääntelyn kokonaisuudessa, joka laajentaa kyberturvallisuuden riskienhallinnan juridiikan puolelle. Tämä tarkoittaa sitä, että toimijat ohjataan tarkentamaan ja kehittämään kyberturvallisuuden riskienhallintaansa sääntelyn edellyttämällä tavalla. Tämä myös osaltaan tarkoittaa sitä, että i) jatkossa riskienhallintaa käsitteleviin tiimeihin kutsutaan (tai liittyy mukaan oma-aloitteisesti) yhä enemmän juristeja ja ii) riskienhallintaa valvotaan tarkemmin toimijan johdon ja valvontaviranomaisten toimesta. Lopulta tavoitteena on luoda turvallisemmat palvelut ja yhteiskunta meille kaikille.

TIIVISTELMÄ KESKEISESTÄ EU:N KYBERTURVALLISUUSSÄÄNTELYSTÄ:

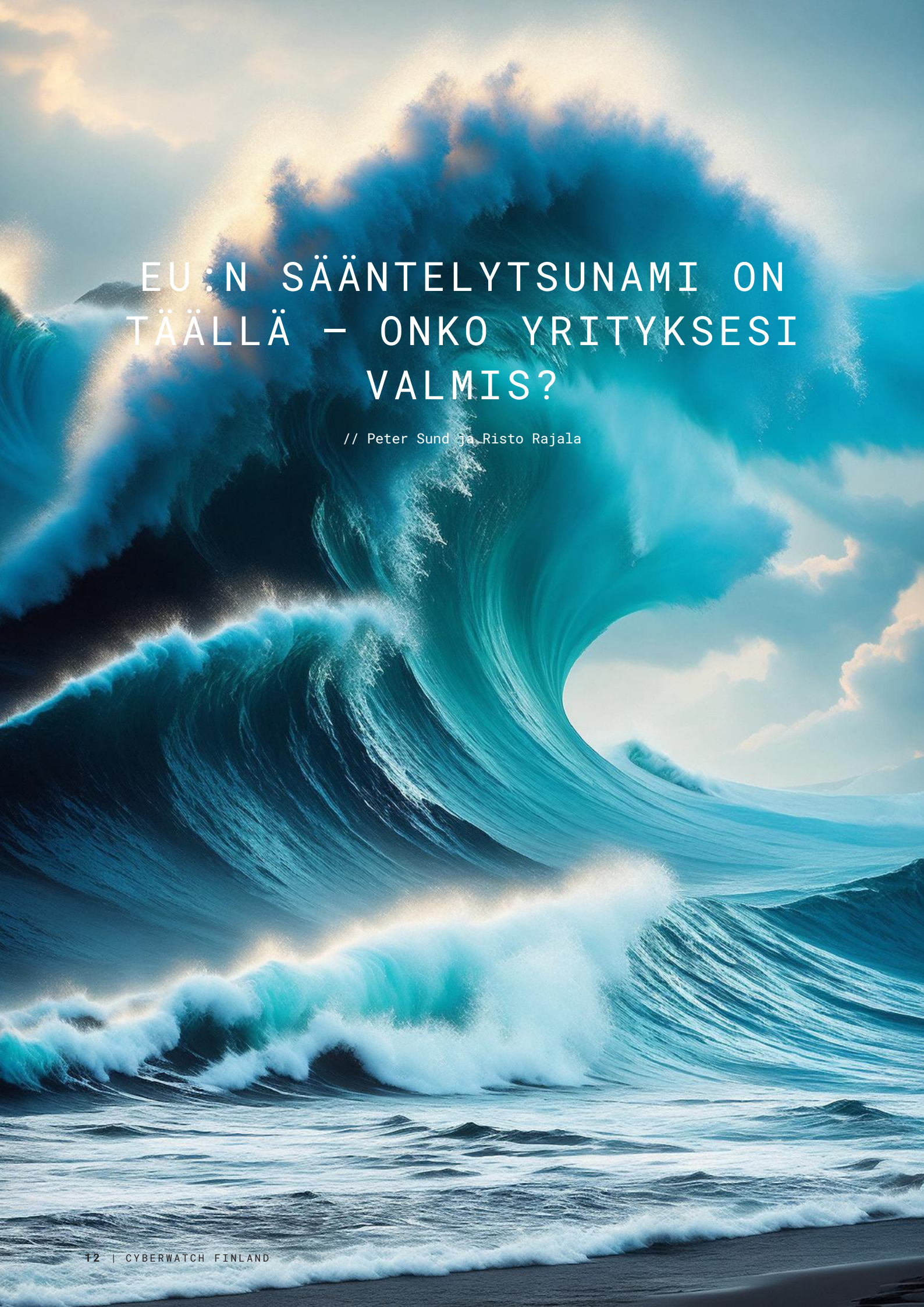
- EU:n yleinen tietosuoja-asetus ("GDPR") (EU) 2016/679 (sovellettavana)
- Kyberturvallisuusasetus (EU) 2019/881 (sovellettavana)
- Kyberturvallisuusdirektiivi ("NIS2") (EU) 2022/2555 ja sen implementoiva kansallinen lainsäädäntö (soveltaminen 18.10.2024 alkaen)
- CER-direktiivi (EU) 2022/2557 ja sen implementoiva kansallinen lainsäädäntö (soveltaminen 18.10.2024 alkaen)
- Finanssialan digitaalisesta häiriönsietokyvystä annettu asetus ("DORA") (EU) 2022/2554 (soveltaminen 17.1.2025 alkaen). ■

JOHANNA TUOHINO

- Senior Associate
- Johanna Tuohino on erikoistunut kyberturvallisuuteen, tietosuojaan, sähköiseen viestintään ja teknologiaan liittyvään regulaatioon. Johanna on Dittmar & Indreniuksen Cyber Security -tiimistä vastaava juristi.
- **Dittmar & Indrenius**

JOONA LINNER

- Associate, asianajaja, CIPP/E, Certified Digital Asset Advisor (CDAA)
- Joona Linner on erikoistunut kyberturvallisuuteen, tietosuojaan, fintechiin ja teknologiaan liittyvään regulaatioon. Joona on yksi Dittmar & Indreniuksen Cyber Security -tiimin kantavista voimista.
- **Dittmar & Indrenius**



EU:N SÄÄNTELYTSUNAMI ON TÄÄLLÄ – ONKO YRITYKSESI VALMIS?

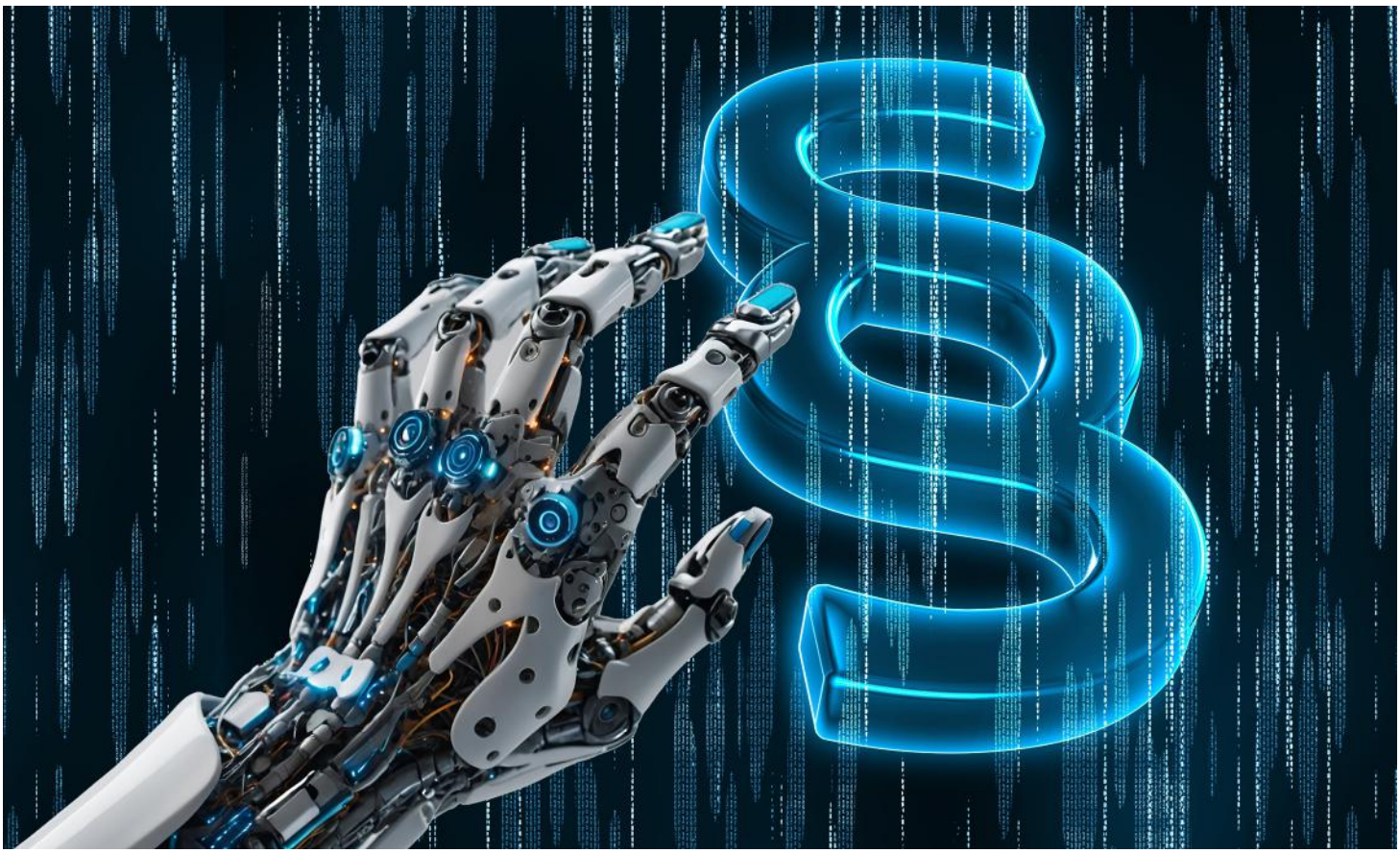
// Peter Sund ja Risto Rajala

Euroopan unionilla on kunnianhimoinen tavoite rakentaa parempaa digitaalista elämää eurooppalaisille. Tavoite ei kuitenkaan ole mikään "Euroopasta tullut" ajatus, vaan meidän kaikkien demokraattisesti määritellyn yhteisen tahtotila. Keinoksi tavoitteen saavuttamiseen se on valinnut sääntelyn, koska siihen EU kykenee paremmin kuin moni muu. Vaikka yritykset eivät yleisesti ottaen toivokaan lisääntyvää sääntelyä, digitalisaation, datatalouden ja digitaalisten markkinoiden lupaukset ovat liiketaloudellisesti sekä taloudellisen hyvinvoinnin osalta ohittamattomat.

Menneellä vaalikaudella 2019–2024 Euroopan komissio esitti kymmeniä digitaaliseen elämäämme eri tavoin vaikuttavia säädösehdotusta ja moni näistä on jo läpäissyt tai pian läpäisemässä EU:n neuvoston ja Euroopan parlamentin lainsäädäntöprosessit. Merkittävästi lisääntyvä sääntely on herättänyt paljon keskustelua, myös huolta ja kritiikkiä. Usein kuulee puhuttavan sääntelytsunamista, eikä väite ole täysin harhaanjohtava. Tsunami – joka ei siis ole yksittäin suuraalto, vaan sarja lukuisia aaltoja – on juuri saavuttamassa digitaalisesti toimivien yritystemme "rannan". Samalla lienee paikallaan kysyä, montako ei-digitaalista työnantajayritystä Suomessa ylipäätään on? Mullistuksesta selviävät voittajina ne yritykset, jotka onnistuvat ratsastamaan sääntelyaallon harjalla, eli omaksumaan uudet velvoitteet ketterästi, eli nopeasti ja kustannustehokkaasti, siten sopeuttamaan liiketoimintansa niiden asettamiin reunaehtoihin.

Digitaalista liiketoimintaa harjoittavien yritysten näkökulmasta olennaisimpia uusista laeista ovat tekoälyasetus, data-asetus, NIS2-direktiivi ja kyberkestävyyssäädös. Käytännössä kaikkien näiden neljän lain sisältö on tiedossa ja merkittävin huomio kohdistuu niiden osalta jo toimeenpanovaiheen käynnistämiseen. Myös muilla hyväksytyillä tai vielä valmistelussa olevilla säädöksillä tulee olemaan vaikutuksensa, mutta useimmiten sektorikohtaisella tai pistemäisellä tavalla verrattuna edellä mainittuihin, soveltamisaloiltaan erittäin laajoihin lakeihin.

EU:n tekoälyasetus, eli Artificial Intelligence Act (AI Act), on ensimmäinen laaja sääntelykehys tekoälylle maailmassa. Sen tavoitteena on varmistaa, että tekoälyjärjestelmät ovat turvallisia ja täyttävät eurooppalaisen perusoikeusnormien vaatimukset, kuitenkin samalla edistäen innovaatioita. Tämä hienohkolta vaikuttava tavoite tarkoittaa käytännössä, että innovaatiot kohdistetaan hyväksyttävien käyttötapausten alueelle, eikä esimerkiksi sellaisiin, joita Kiinassa käytetään kansalaisten läpitunkevaan valvontaan ja kontrollointiin. Asetus luokittelee tekoälyjärjestelmät riskitason mukaan ja asettaa tiukemmat vaatimukset korkean riskin sovelluksille, kuten terveydenhuollossa ja liikenteessä käytettäville järjestelmille. Lisäksi se kieltää kokonaan tekoälyn tietyt käyttötarkoitukset, kuten reaaliaikaisen biometrisen tunnistamisen julkisilla paikoilla, ellei kyseessä ole vakava turvallisuusuhka. Tekoälyasetus astui voimaan elokuussa 2024 ja sitä aletaan soveltamaan erilaisten siirtymäaikojen puitteissa pääosin vuonna 2026.



EU:n data-asetus, eli Data Act pyrkii parantamaan datan saatavuutta ja käyttöä Euroopassa. Sen tavoitteena on varmistaa, että dataa voidaan jakaa reilusti ja avoimesti, edistää innovaatioita ja luoda kilpailukykyinen datamarkkina. Tässä keskiössä on dataa tuottavan ICT-teknologian loppukäyttäjien oikeus omaan käytönaikaiseen dataansa. Asetus koskee erityisesti verkkoon liitettyjä laitteita ja palveluita, ja se pyrkii helpottamaan näiden tuottaman datan hyödyntämistä. Data-asetus astui voimaan tammikuussa 2024 ja sen soveltaminen alkaa pääosin syyskuussa 2025.

NIS2-direktiivi pyrkii vahvistamaan kyberturvallisuutta yhteiskunnan toiminnan kannalta tärkeillä aloilla ja toiminnoissa, kuten energiateollisuudessa ja terveydenhuollossa. Direktiivi edellyttää organisaatioita ottamaan käyttöön tehokkaita riskienhallintakeinoja ja raportoimaan kyberturvallisuuspoikkeamista koko unionin kyberturvallisuustason nostamiseksi. Suomessa hallitus on direktiivin toimeenpanemiseksi laatinut esityksen kyberturvallisuuslaiksi, joka on parhaillaan Eduskunnan käsittelyssä. On kuitenkin todennäköistä, ettei laki ole vielä voimassa 18.10., jolloin NIS2-direktiivi soveltaminen alkaa koko EUalueella. Tilanne, jossa EU-tasolla annettu direktiivi on voimassa, mutta kansallinen laki ei, on direktiivin soveltamisalaan kuuluvien yritysten näkökulmasta haastellinen ja luo epävarmuutta toimintakenttään. Onkin tärkeää, että Suomessa säädettävä laki saadaan voimaan mahdollisimman pian. Kyberala on julkaissut soveltamisalaan kuuluvien yritysten tueksi soveltamisoppaan, josta julkaistaan päivitetty versio, kun laki on lopullisesti hyväksytty. Oppaan valmistelussa on ollut mukana asiantuntijoita useista kymmenistä kyberturvallisuusalan asiantuntijayrityksestä, mikä on mahdollistanut laaja-alaisen huippuosaamisen sekä eri kokemusten hyödyntämisen.

Viimeisenä, mutta mahdollisesti merkittävimpänä, lainsäädäntövalmistelussa on EU:n kyberkestävyyssäädös, eli Cyber Resilience Act (CRA). Kyseessä on soveltamisalaltaan massiiviisen laaja EU-asetus, joka asettaa tietoturvaa koskevat vähimmäisvaatimukset lähes kaikille EU-markkinoilla tarjottaville laitteille ja ohjelmistoille. Kyse on siis digitaalisesta tuoteturvallisuudesta tuotteiden elinkaaren aikana. Asetus pyrkii varmistamaan, että tuotteet tuodaan markkinoille (myös kolmansista maista) ja pidetään valmistajan toimesta käyttöturvallisina. Tuoteturvallisuus tarkoittaa korkeampaa tietoturvallisuutta ja on välttämätön elementti digitaalisessa toimintaympäristössä. EU:n neuvosto ja Euroopan parlamentti saavuttivat sovun asetuksen sisällöstä marraskuussa 2023 ja sen odotetaan valmistuvan lopullisesti vuoden 2024 loppuun mennessä. Asetus astuu asteittain voimaan kolmen vuoden siirtymäajan aikana vuoteen 2027 mennessä.

Kunnianhimoiset uudet säädökset voivat parhaimmillaan tehdä eurooppalaisten digitaalisesta elämästä merkittävästi nykyistä turvallisempaa ja toimivampaa sekä muodostua globaaleiksi normeiksi, joita noudatetaan myös muualla maailmassa. Tämä kuitenkin edellyttää massiivisia panostuksia säädösten yhdenmukaisen ja onnistuneen toimeenpanon varmistamiseen kaikissa EU:n jäsenmaissa. Jos toimeenpano toteutetaan huolimattomasti tai epäoptimaalisesti, tarkoittaa se, että säädöksen tärkeät tavoitteet jäävät saavuttamatta. Samalla yritykset

joutuvat painimaan lisääntyneiden velvoitteiden, hallinnollisen taakan ja pahimmassa tapauksessa vakavien tulkintaepäselvyyksien ja muiden liiketoiminnan edellytyksiä heikentävien haasteiden kanssa. Riittävien panostusten lisäksi on välttämätöntä, että vastuuviranomaiset osallistavat aidosti ja aktiivisesti säädösten soveltamisalaan kuuluvia yrityksiä sekä niiden edustajia mukaan työhön. Uudet säädökset muodostavat varsinkin yhdessä niin merkittävän kokonaisuuden, ettei sitä ole mahdollista hallita pelkästään viranomaisvoimin. Yritykset ja kolmas sektori tarvitaan mukaan laatimaan parhaat keinot täytäntöönpanoon sekä tuottamaan tarvittavat uudet tuotteet ja palvelut.

Varsinkin kyberkestävyyssäädöksen onnistunut kansallinen toimeenpano mahdollistaisi kilpailuetuja suomalaisille yrityksille. Tämä edellyttää, että Liikenne- ja viestintäministeriö yhteistyössä Traficomin kanssa luo aiempaa selkeämpiä kannustimia kolmannen osapuolen hyväksyntää edellyttävien tuotteiden arviointilaitoksiksi soveltuville yrityksille ja hyväksyy niitä ennakoivasti riittävässä määrin. Arviointilaitoksista hyötyvät erityisesti suomalaiset vientiyritykset, jotka saisivat asetuksen soveltamisalaan kuuluvat tuotteensa EU:n sisämarkkinoille kansainvälisiä kilpailijoitaan luotettavammin ja nopeammin. Viivytyksetön ja laajamittainen laitosten hyväksyntä tarjoaisi myös arviointipalveluyrityksille mahdollisuuden tarjota palveluita koko EU-alueella toimiville laite- ja ohjelmistovalmistajille sekä maahantuojille. Näin Suomessa toimiva kyberturvallisuusteollisuuden ekosysteemi vahvistuisi, sekä työllisyys ja verotulot lisääntyisivät. Riskiperusteisen vaatimustenmukaisuuden arvioinnista ei saa muodostua hidastetta kotimaisten tuotteiden markkinoillepääsylle. Yli puolelle Suomen suurimipien pörssiyhtiöiden sekä valtavan määrän PK-yritysten tuotteista kohdistuu asetuksen myötä uusia teknisiä vaatimuksia. Mikäli arviointilaitoksia ei ole riittävästi, ovat vaikutukset suomalaiselle elinkeinoelämälle ja siten kansantaloudelle hyvin vahingolliset. Sidosryhmien osallistaminen ja tarpeiden huomioiminen toimeenpanon eri osa-alueilla vahvistaa onnistumisen edellytyksiä merkittävästi.

Liikenne ja viestintävirasto Traficom on avainasemassa uusien EU-säädösten kansallisen toimeenpanon toteuttajana. Julkisen talouden sopeutustarpeiden lisääntyessä Traficomin ja muiden olennaisten virastojen tehtäviä on tarpeen arvioida ja tarkentaa ja niille varattujen resurssien kohdentamisessa on priorisoitava erityisesti kyberkestävyyssäädöksen ja muun EU-sääntelyn toimeenpanoon liittyviä tehtäviä. EU-sääntelyn kansalliseen toimeenpanoon liittyvillä toiminnoilla on huomattavia kerrannaisvaikutuksia yhteiskunnan toimintaan ja kotimaisen elinkeinoelämän toimintaedellytyksiin, ja siten työllisyyteen ja talouskasvuun. Liikenne- ja viestintäministeri Lulu Ranne lupasi syyskuussa järjestetyssä Liikenne- ja viestintäfoorumissa, että uuden EU-sääntelyn toimeenpano toteutetaan talouskasvua tukevalla tavalla. Ajatus elinkeinoelämän näkökulmasta erittäin kannatettava, mutta samalla on pidettävä mielessä, että kasvua tukeva toimeenpano edellyttää, että siihen kohdistetaan todellista huomiota.

Kyberala on osallistunut aktiivisesti kaikkiin vaiheisiin uusien EU-säädösten elinkaaren aikana. Vaikutimme yhdessä kattojärjestömme Teknologiateollisuus ry:n kanssa aktiivisesti erityisesti NIS2-direktiivin ja kyberkestävyyssäädöksen sekä tekoälyasetukseen ja data-asetukseen valmisteluun Euroopan komission, Euroopan Parlamentin ja valtioneuvoston osalta. Nyt teemme aktiivista yhteistyötä viranomaisten kanssa säädösten kansallisen toimeenpanon tukemiseksi ja mobilisoimme yhdistyksemme jäsenorganisaatioita mukaan tähän työhön. Neuvomme mielellämme jäsenorganisaatioita ja kumppaneitamme uusiin EU-säädöksiin liittyvissä kysymyksissä ja tarjoamme tietoa niiden toimeenpanoon liittyvistä mahdollisuuksista. Tässä työssä käytössämme ovat myös Teknologiateollisuus ry:n voimavarat. ■

PETER SUND

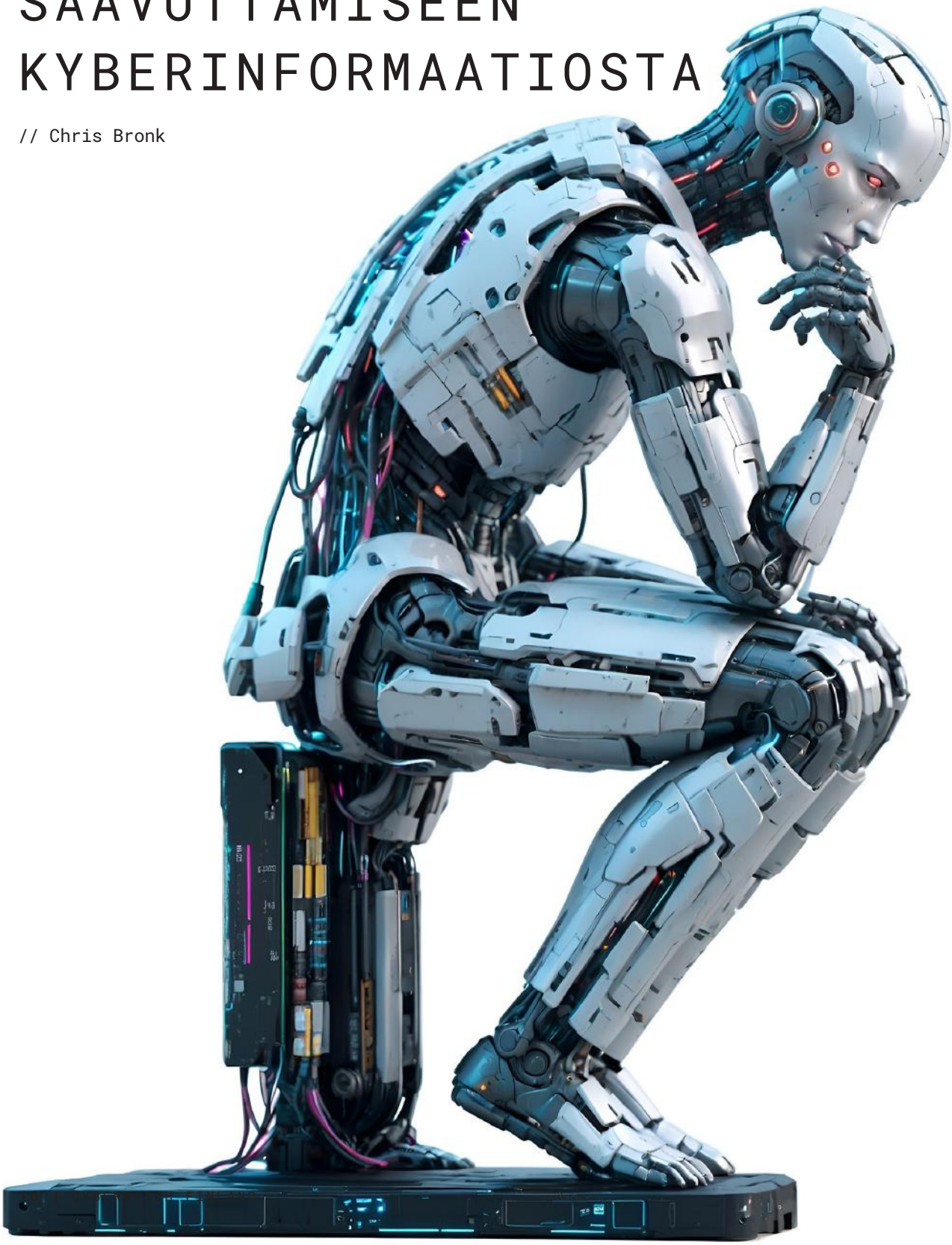
- Kyberala ry:n (FISC ry) toimitusjohtaja
- **Teknologiateollisuus ry**

RISTO RAJALA

- Kyberala ry:n (FISC ry) neuvonantaja
- **Teknologiateollisuus ry**

AAVISTUKSISTA ENNUSTUKSIIN: IHMISEN JA KONEEN ÄLYKKYYKSIEN YHDISTÄMINEN SEKÄ TILANNEYMMÄRRYKSEN SAAVUTTAMISEEN KYBERINFORMAATIOSTA

// Chris Bronk



TIIVISTELMÄ: Hybridisodankäynnin operaatiot sisältävät "kaikki, millä saavutetaan tuloksia" -strategian, mukaan lukien merkittävät informaatio-operaatiot. Länsimaisten demokratioiden on ymmärrettävä paremmin niitä vastaan toteutettavia informaatio-operaatioita. Tähän on sisällytettävä Internetin välityksellä suunnattujen pahantahtoisten poliittisten kampanjoiden tarkempi havaitseminen, seuranta ja mittaaminen.

JOHTOPÄÄTÖKSET: Jotta voidaan tutkia puolustusvaihtoehtoja, jotka kunnioittavat demokraattisia arvoja ja ihmisoikeuksia, tarvitaan käyttäjäkeskeisiä toimintoja, jotka voivat maksimoida tuen ja minimoida inhimilliset virheet, joihin liittyy valinnanvapaus soveltaa sitä yksilötasolla.**:** Tiedon voiman ja sillä tapahtuvan vaikuttamisen teorioita voidaan testata ja optimoida kehittyvällä tekniikalla Internet-tietovirtojen ja muiden niihin liittyvien ilmiöiden havainnoinnilla. Tätä toimintaa on toteutettava laajassa mittakaavassa ja avoimesti, jotta demokraattisia yhteiskuntia voidaan suojella paremmin pahantahtoisilta vaikuttamiskampanjoilta. Tällaisella toiminnalla saadaan lisähyötyjä tiedustelutietojen keruusta ja analysoinnista.

TUTKIMUSKYSYMYS: Miten hybridi-informaation vaikutusta konfliktitilanteissa voidaan havaita, seurata ja torjua?

JATKOTOIMENPITEET: Avoimimmat yhteiskunnat ovat todennäköisesti kaikkein haavoittuvimpia tietojen manipuloinnille ja informaatio-operaatioille. Demokraattisten valtioiden yhteisön on rakennettava puolustus kyberavaruuden kautta välitettävää pahantahtoista informaatiovaikutusta vastaan.

INFORMAATIOVAIKUTTAMISEN MUUTOS

Yli kahdeksankymmentä vuotta sitten brittiläinen diplomaatti, toimittaja ja akateemikko Edward Hallett Carr julisti kirjassaan The Twenty Years' Crisis, että valtaa voidaan käyttää kolmella alueella – sotilaallisella, taloudellisella ja informaatiolla. [1] Korvaten Carrin termin pehmeä valta mielipiteen vallalla Nye tuotti samanlaisen arvion kuusi vuosikymmentä myöhemmin.[2] Vaikka harjoittajat ja tutkijat voivat olla yhtä mieltä siitä, että informaatiovoima on tärkeää, lainaten Simonilta, on kysyttävä: "Missä määrin havainnon ja mittaamisen operatiiviset hyödyt ovat meidän käytettävissä?" [3] Geopoliittisen informaatioympäristön tutkijoiden ja ammattilaisten tehtävänä on tunnistaa, miten nopeasti kehittyviä tietolähteitä voidaan käsitellä ja analysoida uusilla laskennallisilla menetelmillä, joita kutsutaan tekoälyksi (AI).

MIKÄ LISÄÄ TILANNETIETOISUUTTA HYBRIDIKONFLIKTEISSA?

Resilientti ja tarkka tilannetietoisuus hybridiuhista on riippuvainen hybridiareenan kunkin osa-alueen havainnoinnista ja mittaamisesta, mikä yhdistää "valtiollisen konfliktin tappavuuden epäsäännöllisen sodankäynnin fanaattiseen ja pitkittyneeseen kiihkoon". [4] Tällainen havainto tarkoittaa vastustajan monentyyppisen toiminnan seurantaa. Hallitukset ja muut toimijat ovat luoneet erilaisia havainto- ja mittausvalmiuksia sosiaalisesta mediasta ja pankkijärjestelmistä tietokoneverkkoihin ja tiedustelusatelliitteihin. Tämä uusi valtioiden välisen konfliktin muoto on erotettu kylmän sodan haalistuvista muistoistamme siinä, että siinä missä tietoa oli kerran vaikea löytää, on sitä nyt usein liikaa. [5] Esiin nousee kuitenkin uusia kysymyksiä. Ilmiöiden mittaamiseen voidaan käyttää riittävän laadukasta dataa, jonka mittaaminen on keskeinen askel tilannetietoisuuden kannalta. [6]

Tietokoneiden yleistyminen ja tietojenkäsittelyn kehittyminen ovat antaneet ihmiskunnalle suuremman kyvyn kehittää kvantitatiivisia mittareita kaikenlaisille ilmiöille. Mobiilit tietokonelaitteet tarjoavat laajasti tietoja kuvista maantieteelliseen sijaintiin. [7] Helmikuun 2022 hyökkäyksen alkaessa Ukrainaan sosiaaliseen mediaan tulvi kuvia sotatoimista, jotka oli otettu suurelta osin mobiililaitteista. [8] Avointen lähteiden tiedusteluanalyytikot, enimmäkseen amatöörit, kävivät läpi videoita ja kuvia taisteluista luodakseen kuvan sotilaallisesta toiminnasta.[9]

Mitä tulee eri lähteistä saatavien tietojen yhdistämiseen strategisella tasolla ja niiden muuntamiseen operatiiviseksi toiminnaksi, tärkeimmät kysymykset ovat tarkkuus ja niiden analyysin oikea-aikaisuus. Esimerkki menestyksestä tällä alalla on Ukrainan ohjusisku Berdianskin satamaan maaliskuussa 2022. [10] Venäjä julkaisi propagandavideon operaatioistaan merisatamassa, mikä mahdollisti Ukrainan tarkan kohdistamisen siellä oleviin venäläisiin maihinnousualuksiin. Ukrainan ohjusisku upotti sitten yhden aluksista ja vaurioitti pahasti kahta muuta. [11] Tämä OSINT-muoto voi olla erittäin hyödyllinen; Sen sisällyttäminen nopeaan, tehtäväkeskeiseen tiedusteluanalyysiyritykseen tuo kuitenkin mukanaan haasteita – eikä vähiten sen, että varovainen ja siitä tietoinen vihollinen voi tarkoituksenmukaisesti tuottaa disinformaatiota OSINT-analyysiä sotkemaan.

Hallituksen, teollisuuden ja yksilöiden käytettävissä oleva tiedustelutilannekuva eroaa suuresti siitä, mitä se oli viime suurvaltakilpailun aikana, joka päättyi Neuvostoliiton hajoamiseen. [12] Tieto- ja viestintätekniikan valtava teknologinen kehitys on uudistanut tiedustelutoiminnan täysin. Ulkomaisia agentteja voidaan rekrytoida chat-huoneissa syrjäisten kujien sijaan. Ylätason tilannekuva, joka oli aikoinaan saatavilla vain suurvalloille, on nyt saatavilla kaupallisesti lataamalla Internetistä. Arkisto-

kaappeihin ei tarvitse murtautua, kun tietokoneilla säilytettävä data voidaan varastaa jopa toiselta puolen maapalloa. Tiedustelutiedon kerääjille on olemassa eräänlainen runsaudenpula. Kuitenkin tämän ”digitaalisen pakokaasun” [13] arvo tunnustetaan vasta sen jälkeen, kun tiedot on onnistuneesti muutettu toiminnaksi – verkkosensuurista tykistöpommituksiin. Viestinnän vallankumous on kaksiteräinen miekka korkean teknologian yhteiskunnille ja niiden korkean teknologian armeijoille.

Ei ole epäilystäkään siitä, etteivätkö matkapuhelimet, jotka ovat korvanneet kaiken laskimista ja kameroista mediastudioihin ja taskulamppuihin, olisi vaikuttaneet valtavasti ihmiskuntaan. [14] Matkapuhelinliittymien määrä ylitti maailman väestön joskus vuosien 2015 ja 2020 välillä. [15] Ruotsalainen Ericsson, matkaviestintää ylläpitävän teknisen infrastruktuurin rakentaja, väittää, että noin 60 prosentilla maapallon väestöstä on älypuhelin. [16] Vuosina 2023–2024 näiden laitteiden ja muiden tieto- ja viestintätekniikan infrastruktuurien välillä kulkevan datan määrä kasvoi 25 prosenttia. [17]

Haittapuolena on, että näitä laitteita voidaan seurata ja valvoa tekniikoilla, jotka skannaavat sähkömagneettista spektriä ja tarkastavat runkoverkkojen tietovirtoja. Niitä vastaan on kehitetty myös hakkerointityökaluja, jotka vaarantavat sovellukset ja käyttöjärjestelmän ohjelmistot. Venäjän ja Ukrainan sodan taistelukentillä matkapuhelinten on osoitettu olevan valtava riskitekijä. Konfliktin etulinjassa olevien/taistelevien laitteiden yhdistäminen matkapuhelinverkkoon on ollut usein hyökkäyksiä laukaiseva tekijä, ja tämä on pitänyt paikkansa jo vuosikymmenten ajan. [18] Vahva todiste mobiililaitteiden haavoittuvuudesta on se, että venäläisten pienten yksiköiden komentajien on havaittu naulaavan matkapuhelimia bunkkereiden seiniin mikäli niitä löytyy joukoilta, kuten yhdessä viraalivideossa tapahtui.

Kuva: Venäläinen sotilas naulaa takavarikoituja matkapuhelimia tolppaan vuonna 2024. Lähde: @clashreport, x.com.

Yksi Venäjän ja Ukrainan sodan yllättävimmistä kehityskuluista on kaupallisen internetin ja matkapuhelinteknologian käytettävyys taistelukentällä. Se, että tykistötuli kutsutaan Starlink-satelliittimodeemin kautta, on vain yksi konfliktin odottamattomista tapahtumista. Hybridi- tai "harmaan vyöhykkeen" konflikteiksi tunnistettujen toimintojen seuraaminen yhdistää tietoja useilta alustoilta ja järjestelmistä. [19] Hybridikonfliktien ontologiaan kuuluvat: propagandaoperaatiot, pääasiassa verkossa; viralliset ilmoitukset ja lehdistötiedotteet; kyberhyökkäykset ja -puolustustoiminta; tiedot sotilaallisista liikkeistä ja harjoituksista; ja taloudelliset tiedot (esim. polttoaineiden ostaminen sotaan valmistautumiseksi tai markkinoiden manipulointi epäsymmetrisen edun luomiseksi). Kuten kylmän sodan alkuaikoina, akuuttien turvallisuusongelmien kanssa painivien valtioiden tavoitteena on välttää yllätyksiä. [20] Sen välttäminen tarkoittaa nykyään sitä, että kapasiteettia on lisättävä analysoitaessa sitä tietotulvaa, jota kutsumme tiedustelutiedoksi.

HYBRIDIVAIKUTUKSEN JA -TOIMINNAN MITTAAMINEN

Aikana, jolloin tekoäly (AI) kehittyy nopeammin kuin ikinä, ihmisen kyky ymmärtää tietoa on edelleen huomiokyvyn ja ajan rajoittama. Yhdeltä ihmiseltä kestäisi 200 000 vuotta lukea pelkästään maailmanlaajuisen verkon (www) tietomäärä. Hyvä uutinen mahdollisille hybridisodankäynnin analyytikoille on, että kaikkea ei tarvitse lukea, ja sen tarvitse voidaan saavuttaa ammattimaisella toiminnalla. Analytiikkatiimit voivat seurata informaatio-operaatioiden kannalta olennaisia muuttujia, mutta kysymys kuuluu, miten. [21] Vastaus on kolmikantainen, ja siihen sisältyy a) keskeisten muuttujien tunnistaminen; (b) "normaalin" toiminnan perustason; ja c) eri muuttujien painotukset koneoppimisalgoritmissa kerättyjen tietojen käsittelyssä. Tästä voi syntyä kehys informaatiovallan käytön muutoksen havainnointiin.

Hybridikonfliktin ymmärtäminen edellyttää moninaisten osaamisalueiden yhdistämistä. Suuri osa sisältyy siihen, mitä nykyiset länsimaiset sotateoreetikot kutsuvat informaatioympäristöksi. [22] Rajojen asettaminen tälle ympäristölle on pelottavaa. Se on suuri, aivan kuten fyysinen ympäristö, jossa se on rakennettu. Suuri osa ihmisten vaihtamasta ja omaksumasta tiedosta on digitaalista. Tämä tuottaa valtavia tietovirtoja ja tietovarastoja. Haasteena on löytää ne lähteet, jotka voivat paremmin valaista vallankäyttöä kansainvälisessä järjestelmässä. Kansainvälisessä akateemisessa ympäristössä tietoulottuvuutta on lähestytty menetelmillä uutisanalyysi,[23] julkilausuntoanalyysi,[24] johtajuusanalyysi ja siihen liittyvä poliittinen psykologia,[25] ja jo jonkin aikaa Internet-viestinnän ja vuorovaikutuksen analyysillä. [26] Mooren lain

ansiosta laskentatehon kasvussa näiden alojen tutkimusmekanismeja voidaan suunnitella uudelleen tekniikan kehityksen valossa. [27]

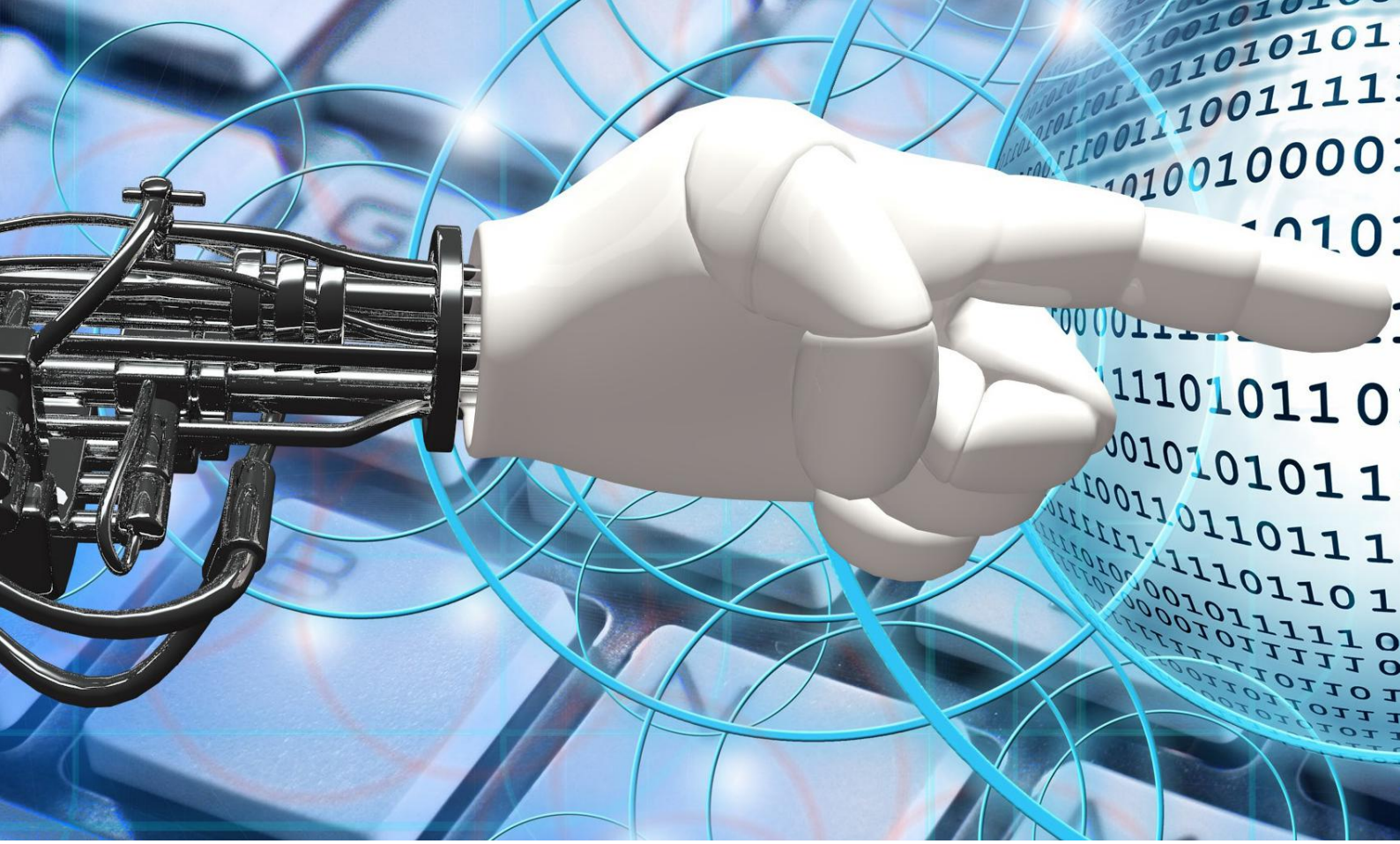
Hybridisodankäynnin informaatioympäristössä on rakennettava silta teknisen kapasiteetin ja yhteiskunnallisen reagoinnin välille. Mainonta voi tarjota oikotien informaatiovallan arvostamiseen kansainvälisessä kilpailussa ja konflikteissa. [28] Teknologia on mullistanut mainosalan. Kaikkialla läsnä olevan tietojenkäsittelyn saapuessa Internet-yritysten, kuten Alphabetin (Google) ja Metan (Facebook), toimittamat mainokset kohdistuvat yksilöihin eikä yleisöihin. [29] Poliittisen mainonnan menojen ennustetaan nousevan Yhdysvalloissa lähes 3,5 miljardiin dollariin vuoden 2024 vaalisyklillä, kun taas perinteiset mainosmenot (TV, radio, painettu jne.) ovat edelleen paljon enemmän, noin 7,9 miljardia dollaria. Kokonaismäärä, noin 12 miljardia dollaria, on lähes kolmanneksen enemmän kuin vuoden 2020 vaalisyklissä. Suurin osa tästä kasvusta tapahtuu digitaalisen mainosalan piirissä,[30] mikä on polku tietovoimamuuttujien löytämiseen.

Poliittisen mainonnan menojen suurin kasvualue on se, mitä mainosala kutsuu yhdistetyksi televisioksi (Connected TV). Tällä käsitteellä tarkoitetaan internetin välityksellä välitettävää videoa. [31] Alphabetin, Amazonin, Netflixin ja Disneyn kaltaisten perinteisten mediayhtiöiden palvelut toimittavat nämä mainokset katsojille. Ne näkyvät kasvavana videotulvana, ja esimerkiksi Alphabetin YouTube-palveluun ladataan noin 20 päivän edestä videota joka minuutti. Tässä eksponentiaalisesti kasvavassa videoarkistossa propagandistit toimittavat viestinsä yleisölle ulkomailla. [32] Mielenkiintoista on, että Venäjän hallitus esti äskettäin kansalaistensa pääsyn palveluun. [33] Vaikuttaa todennäköiseltä, että sekä videosisältö että sitä ympäröivät mainokset ovat mahdollinen uhka joillekin valtioille. Näitä digitaalisen datan rajoituksia tulisi seurata myös hybridikonflikteja tarkkailevien tahojen toimesta.

X:ssä (entinen Twitter), Telegramissa ja Alphabetin Instagramissa tiedonkeräystä harjoittavien on seurattava monia muuttujia, mukaan lukien näiden alustojen tuottamat metatiedot. [34] Hallitusten virkamiehet ja poliittiset ehdokkaat käyttävät näitä Internet-alustoja viestiensä välittämiseen. [35] Propagandistit ovat jonkin verran vähemmän avoimia siitä, mitä narratiivien levittämisellä tavoitellaan, mutta käyttävät silti samoja työkaluja. [36] Kun aikanaan propagandan levittäminen oli rajoittunut salaa julkaistaviin aikakausilehtiin ja uutiskirjeisiin, on nykyisin työkaluina verkkouutiset ja mielipideblogit,[37] jotka usein tuotetaan suurten tekoälyä hyödyntävien kielimallien (LLM) avulla. [38] Hybridikonfliktien tilannetietoisuus tarkoittaa uskomuksiin ja käsityksiin vaikuttavien tietolähteiden tehokasta seurantaa. Tällaista toimintaa on todennäköisesti harjoitettava lähitulevaisuudessa. Informaatiovoima näyttää säilyttävän merkityksellisyytensä.

MITEN VAIKUTTAMINEN TOIMII HYBRIDIVAIKUTTAMISESSA?

Jotta voidaan ymmärtää, toimivatko vaikutusoperaatiot, voidaan käyttää esimerkkinä Venäjän yrityksistä eristää Ukraina ja riistää siltä lännen tuki. Ennen kuin Yhdysvaltain kongressi äänesti huhtikuussa 2020 Ukrainalle annettavan suuren avustuskierroksen hyväksymisestä, Venäjän propaganda viivytti kuukausien ajan Yhdysvaltojen lainsäädäntötoimia sotilaallisen avun antamisesta Ukrainalle. Äskettäinen Breitbartin otsikko: "Yksinoikeudella: [Puhemies] Johnsonin ylin poliittinen neuvonantaja on entinen lobbaaja ... Asiakkailla on yritysten intressi Ukrainan sotaan", toimii esimerkkinä



informaatio-operaatioista, jossa Venäjä-mielinen toiminta on naamioitu yritysvastaiseen narratiiviin. [39] Potkut saanut Fox News -kommentaattori Tucker Carlson haastatteli Vladimir Putinia Venäjällä ja esiintyi videoklipeissä, joissa hän kutsui Moskovaa "paljon mukavammaksi kuin mikään muu kaupunki maassani". [40] Yksi Yhdysvaltain kongressin pitkäaikainen republikaanijäsen nuhteli omaa vaalipiiriään siitä, että Venäjän propagandan esiin nostamia keskustelunaiheita tuotiin jatkuvasti faktoina kamarin keskusteluihin. [41]

Hybridikonfliktisuuntautunut propaganda kohdistuu myös kohdemaiden kansalliseen politiikkaan ja asevoimiin. [42] Käytännössä tämä tarkoittaa niiden ideologista yhteensopivuutta sellaisten operaatioiden kanssa, joihin voidaan kohdistaa valtavaa poliittista propagandaa. Valheelliset raportit Liettuassa palvelevien saksalaisten sotilaiden väkivallasta voivat olla vain jäävuoren huippu Venäjän harjoittamassa Naton vastaisessa digitaalisessa propagandassa. [43] Ehkä paras indikaattori sen tehokkuudesta on uusfasististen elementtien esiin nouseminen Naton asevoimissa ja näihin ryhmiin kuuluvien halukkuus työskennellä omia kotimaitaan vastaan kyberympäristössä levitetyn pahantahtoisen ulkomaisen informaatiovaikutuksen rohkaisemina.

Vaikka covid-19-pandemia ei ollut sotilaallinen konflikti, se avasi ovet propagandisteille, myös Yhdysvalloissa, manipuloida yleisöä verkossa. [44] Valheelliset narratiivit harhaanjohtivat naivia ja helposti manipuloitavaa väestönosaa. Joissakin tapauksissa seurauksena oli jopa kuolema. Tietoympäristössä on runsaasti hybridikonflikti-indikaattoreita, mutta niiden läsnäolo ei välttämättä anna ennustetta tulevasta sotilaallisesta konfliktista tai peitellystä toiminnasta. Ennakkovaroitus ja rauhanpyrkimykset edellyttävät informaatio-operaatioiden ymmärtämistä juurikin kyseisen konfliktin kontekstissa, joka voi siirtyä "harmaalta vyöhykkeeltä" merkittäviin vihollisuuksiin. Tämä tarkoittaa myös sitä, että pelkkä kahden valtion välinen retoriikka ei välttämättä johda avoimeen konfliktiin. Esimeriksi nyt lievennetty Japanin ja Etelä-Korean välinen sanasota oli indikaatio pitkään jatkuneesta vihamielisyydestä, mutta ei uudesta konfliktista.

TEKOÄLYN ROOLI TILANNEYMMÄRRYKSEN SAAVUTTAMISESSA DATAMERESSÄ

Tieto- ja viestintätekniikka on muuttanut yhteiskuntaa erityisesti tiedon nopean leviämisen kautta. Ehkä tärkein havainto tämän kirjoituksen valmistelussa oli usein toistettu usko siihen, että tekoäly vastaa kaikkiin kysymyksiin ja poistaa kriittisen ajattelun tarpeen. [45] Tällä voi olla tuhoisia vaikutuksia, kun opimme lisää siitä, miten tekoälyn suorituskyky voi olla puolueellinen ja miten tähän puolueellisuuteen voidaan vaikuttaa. [46]

Käsillä on valtava laskentakapasiteetti digitaalisen tiedon ymmärtämiseen. Tietojen käsittelytekniikat voivat olla uskomattoman hyödyllisiä järjestyksen tuomisessa tietoympäristön kaaokseen. [47] Esimerkiksi BERT, laskennallis-lingvistinen työkalu, voidaan kouluttaa havaitsemaan verkkopropaganda jatkuvasti kehittyvän kielellisen mallinsa avulla. [48] Propagandistit innovoivat jokaisesta edistysaskeleesta, joka tehdään informaatio-operaatioiden havaitsemiseksi. Tämä on teknologisesti tuetun valtiollisen kamppailun luonne. Kun kansainväliset

toimijat jakautuvat osapuoliin, on käynnissä jatkuva kilpailu uusien innovaatioiden hyödyntämisessä suhteellisen edun saavuttamiseksi.

Hybridikonfliktin informaatiokomponentit ovat löydettävissä, ja tämä voidaan osittain toteuttaa tietokoneilla. Tekoäly ei kuitenkaan ole ihmelääke. Tekoälystä puhuvat ehkä liikaa ne, jotka eivät ymmärrä, miten tekniikka toimii tänään tai kehittyy. Tekoälyksi kutsumamme neuroverkon koneoppimisprosessin kehitys etenee kuitenkin johdonmukaisesti. Googlen tekoälyn tutkimus- ja kehityskeskuksen Deep Mind:n johtaja on vakuuttanut äskettäin, että nämä edistysaskeleet jatkuvat. Hän huomauttaa: "Viime vuosina koneoppiminen on mielestäni todella muuttanut odotuksiamme siitä, mitä ajattelemme tietokoneiden pystyvän tekemään. Jos ajatellaan taaksepäin 10 tai 15 vuotta sitten, puheentunnistus tavallaan toimi, mutta se ei ollut todellakaan saumaton - se teki paljon virheitä. Tietokoneet eivät oikein ymmärtäneet kuvia kuvan pikselitasolta. Luonnollisen kielen käsittelyssä oli paljon työtä, mutta se ei oikeastaan ollut kielen käsitteiden ja monikielisen datan syvällistä ymmärtämistä. Luulen, että *olemme siirtyneet siitä vaiheesta vaiheeseen, jossa tietokoneet todella pystyvät näkemään ja havaitsemaan ympäröivän maailman paljon paremmin kuin 10 vuotta sitten* [tekijän kursivointi]. [49]

Vaikka onkin siis nähtävissä valtavia edistysaskeleita tietokoneiden kyvykkyyksissä, informaatiovaikutuksen tai muiden hybridisodankäyntitaktiikoiden ymmärtäminen vaatii käytännön työkalujen kehittämistä. Yksi lähestymistapa on simuloida yhteiskuntaa suuressa mittakaavassa. Eräs tutkimusryhmä suunnittelee tarkkojen kognitiivisten mallien käyttöä, jotka edustavat tiettyjen yksilöiden ajattelutapaa. [50] Tällaisen lähestymistavan haasteena on kuvata populaation heterodoksinen luonne ja ymmärtää, miten tekoälyllä tehtävä arviointi voi tuottaa hyödyllisiä havaintoja. Tietojenkäsittelyn kehitys jatkuu, mutta suurempi haaste voi olla tietojen jäsentäminen ja painottaminen hyödyllisten analyyttisten työkalujen rakentamiseksi. Tämä prosessi, puhumattakaan hybridisodankäynnistä, on edelleen suhteellisen kehittymätön kansainvälisiin suhteisiin sovellettuna.

SIVIILI- JA DIPLOMAATTISET INSTITUUTIOT KOROSTUVAT

Hybridikonflikti käsittää valikoiman toimia, jotka voivat tuottaa maksimaalisen vaikutuksen samalla kun hallitaan eskaloituvaa dynamiikkaa. Lännen demokratioiden hallitukset käyttävät diplomaattisia, tiedustelu- ja sotilaallisia kykyjä rauhan ylläpitämiseksi ja ennakkovaroituksen tarjoamiseksi tavalla, jota ei ole nähty sitten maailmansotien. Vuodesta 1945 lähtien nämä organisaatiot ovat sopeutuneet moninaisiin haasteisiin disinformaatio-operaatioista ydinsodan uhkaan. Turvallisuuden varmistaminen on vaatinut monien uutta teknologiaa ja innovatiivisia tekniikoita hyödyntävien toimijoiden panosta, jotta on voitu vastata älykkäiden ja motivoituneiden vastustajien menetelmiin.

Tämä mukautus ulottuu myös muutoksiin kansainvälisten suhteiden ”pelisäännöissä”. Syvävääreennökset, kyberhyökkäykset ja kansainväliset rikollisterroristisyndikaatit ovat kaikki nykyisen turvallisuusympäristön

todellisuutta, jotka olisi leimattu tieteiskirjallisuudeksi muutama vuosikymmen sitten. Uusien toimijoiden ja toimien lisäksi konfliktien luonne on muuttunut globaaleiksi pelikentiksi, joissa yritetään saavuttaa etulyöntiasema pitäen eskalaatio kurissa. Merkittävä haaste on edelleen ohjata tietokonealgoritmien huomio tärkeimpien muuttujien löytämiseen ja analysointiin. Vihamieliset ja aggressiiviset valtiot käyttävät käsillä olevia työkaluja. Esimerkiksi Pohjois-Korea on oppinut käyttämään kybertyökaluja toteuttaessaan kautta aikojen ensimmäisen kansallisen reservipankin ryöstön. [51] Vastapuolen innovaatiokyky digitaalisesti yhteen liitetyssä maailmassa tulee säännöllisesti yllätyksenä niiden valtioiden yhteisölle, jotka pyrkivät edistämään yhteisiä etuja ja kollektiivista turvallisuutta luovaa normeihin perustuvaa kansainvälistä järjestystä. Ensisijaisena tavoitteena on oltava pysyä ajan tasalla niistä innovaatioista, joita tekevät jatkuvasti kasvava joukko autoritaarisia hallintoja, jotka ovat myös yhä halukkaampia keskinäiseen yhteistyöhön.

Jos on olemassa aikamme määrittävä ominaisuus, se on se, että yhteiskunnilla on mahdollisuus selviytyä tietovirtojen keskellä samalla ymmärtäen paremmin sitä maailmaa, jota asuttavat. Tietoympäristö kasvaa eksponentiaalisesti. Sen tapahtumien seuraaminen, on useiden eri tieteenalojen harjoittajien tehtävä. Nämä voivat tehdä yhteistyötä ymmärtääkseen mitä turvallisuus edellyttää. Toimittajat, tutkijat ja huolestuneet kansalaiset ovat hybridisodankäynnin informaatio-operaatioiden eturintamassa. Globaalissa lännessä hallitusten ei kuitenkaan pitäisi saada synninpäästöä vain siksi, että nämä toimijat ovat hyviä havaitsemaan ja puuttumaan valeuutisten leviämiseen. Vaikka sotilaalliset liittoumat perustuvat asevoimien yhteistyöhön, läntisten demokratioiden olisi viisasta kasvattaa siviili- ja diplomaattisia instituutioita hybridikonflikteja varten digitaalisella alueella.

Tämä merkitsee todennäköisesti turvallisuuteen liittyvien institutionaalisten tai organisatoristen siilojen murenemista entisestään. Poliisi, tiedusteluorganisaatiot, asevoimat, yritykset ja vapaaehtoiset kansalaiset osallistuvat yhteisen ymmärryksen tuottamiseen hybridikonfliktien leimaamassa maailmassa. Tämän yhteistyön toiminta on kuitenkin vasta pitkän työn alkuvaiheessa. Kenties tärkein kysymys liittyen hybridisodankäynnin ilmiöiden tunnistamiseen on se, mitä niiden estäminen maksaa niille, jotka ovat valmiita uhrautumaan sen puolesta. ■

CHRIS BRONK

Chris Bronk PhD on apulaisprofessori Houstonin University of Houston's Hobby School of Public Affairs yliopistossa. Hän tutkii tieto- ja tietotekniikan keskinäisriippuvuutta kansainvälisiin suhteisiin. Tämän artikkelin sisältämät näkemykset ovat yksin kirjoittajan eivätkä edusta Houstonin yliopiston tai Texasin osavaltion näkemyksiä.

VIITTEET

[1] Edward Hallett Carr, The Twenty Years' Crisis, 1919–1939: Reissued with a new preface from Michael Cox (Springer, 2016).
[2] Joseph S. Nye, The Future of Power, (Public Affairs, 2011).
[3] Herbert A. Simon, 'Notes on the observation and measurement of political power', The Journal of Politics Volume 15, Issue 4 (1953): 500–516.
[4] Sub-areas of hybrid conflict can include cyber activity, terrorism, information operations, international crime, and economic activity. Frank G. Hoffman, 'Hybrid warfare and challenges', in Strategic Studies, 329–337. (Routledge, 2014).
[5] Margret S. MacDonald and Anthony G. Oettinger, 'Information overload', Harvard International Review Volume 24, Issue 3 (2002): 44.
[6] Erhard Rahm and Hong Hai Do, 'Data cleaning: Problems and current approaches', IEEE Data Engineering Bulletin Volume 23, Issue 4 (2000): 3–13.
[7] Zheng Xu, Lin Mei, Kim-Kwang Raymond Choo, Zhihan Lv, Chuanping Hu, Xiangfeng Luo, and Yunhuai Liu, 'Mobile crowd sensing of human-like intelligence using social sensors: A survey', Neurocomputing 279 (2018): 3–10.
[8] Aaron F. Brantly, 'Ukraine War OSINT Analysis: A Collaborative Student Report' (2023).
[9] Generating intelligence from social media was defined almost a decade ago. OSINT has been discussed significantly since the 1990s. Laura K. Donohue, 'The dawn of social intelligence (SOCINT)', Drake Law Review Volume 63 (2015): 1061.
[10] Chris Bronk, Gabriel Collins, and Dan S. Wallach, 'The Ukrainian Information and Cyber War', The Cyber Defense Review Volume 8, Issue 3 (2023): 33–50.
[11] Brent D. Sadler, 'Applying Lessons of the Naval War in Ukraine for a Potential War with China', Backgrounder 3743 (2023): 1–13.
[12] Alex Roland and Philip Shiman, Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983–1993 (MIT Press, 2002).
[13] Ronald J. Deibert, Reset: Reclaiming the Internet for Civil Society (House of Anansi, 2020).
[14] Muhammad Sarwar and Tariq Rahim Soomro, 'Impact of smartphones on society', European Journal of Scientific Research Volume 98, Issue 2 (2013): 216–226.
[15] https://www.weforum.org/agenda/2023/04/charted-there-are-more-phones-than-people-in-the-world/.
[16] The term "äppärät" is borrowed from Gary Shteyngart's Super Sad True Love Story, a 2011 novel set in a dystopian near future where mobile devices were all-consuming of human attention. Sounds crazy. Gary Shteyngart, Super Sad True Love Story: A Novel. (Random House Trade Paperbacks, 2011).
[17] This data traffic growth of 25 per cent a year is a staggering statistic and has held true for more than a decade. Fredrik Jejdling, Ericsson Mobility Report 2024. June 2024.
[18] Chris Bronk and Gregory S. Anderson, 'Encounter battle: Engaging ISIL in cyberspace', The Cyber Defense Review Volume 2, Issue 1 (2017): 93–108.
[19] Michael J. Mazarr, 'Mastering the gray zone: Understanding a changing era of conflict', US Army War College (2015).
[20] Roberta Wohlstetter, Pearl Harbor: Warning and Decision. (Stanford University Press, 1962).
[21] The value of AI technologies for analytic teamwork is in its earliest phases. Lauro Snidaro, 'ChatGPT Act as an Intelligence Officer', In 2023 IEEE International Workshop on Technologies for Defense and Security (TechDefense), 449–454. IEEE, 2023.
[22] Michelangelo Conoscenti, 'The Military's Approach to the Information Environment', in The Routledge Handbook of Discourse and Disinformation (Routledge, 2023), 218–238.
[23] Kalev Leetaru and Philip A. Schrodt, 'Gdelt: Global data on events, location, and tone, 1979–2012', in ISA annual convention, Volume 2, Issue 4: 1–49. Citeseer, 2013.
[24] Gavan Duffy and Brian Frederking, 'Changing the rules: A speech act analysis of the end of the Cold War', International Studies Quarterly, Volume 53, Issue 2 (2009): 325–347.
[25] Margaret G. Hermann and Charles W. Kegley Jr., 'Rethinking democracy and international peace: Perspectives from political psychology', International Studies Quarterly Volume 39, Issue 4 (1995): 511–533.
[26] Charli Carpenter and Daniel W. Drezner, 'International Relations 2.0: The implications of new media for an old profession', International Studies Perspectives, Volume 11, Issue 3 (2010): 255–272.
[27] Mark S. Lundstrom and Muhammad A. Alam, 'Moore's law: The journey ahead', Science Volume 378, Issue 6621 (2022): 722–723.
[28] Garrett A. Johnson, Randall A. Lewis, and David H. Reiley, 'When less is more: Data and power in advertising experiments', Marketing Science Volume 36, Issue 1 (2017): 43–53.
[29] Ritam Dutt, Ashok Deb, and Emilio Ferrara, '"Senator, We Sell Ads": Analysis of the 2016 Russian Facebook Ads Campaign', in Advances in Data Science: Third International Conference on Intelligent Information Technologies, ICIIT 2018, Chennai, India, 11–14 December 2018, Proceedings 3, 151–168. Springer Singapore, 2019.
[30] Trade press publications can offer some interesting insights. The $12 billion ad spend is an amount roughly the size of Guyana's GDP. '2024 Political Ad Spending Will Jump Nearly 30% vs. 2020', EMarketer, 11 January, 2024, https://www.emarketer.com/press-releases/2024-political-ad-spending-will-jump-nearly-30-vs-2020/.
[31] Paul Murschetz, 'Connected television: Media convergence, industry structure, and corporate strategies', Annals of the International Communication Association Volume 40, Issue 1 (2016): 69–93.
[32] Robert W. Orttung and Elizabeth Nelson, 'Russia Today's Strategy and Effectiveness on YouTube', Post-Soviet Affairs Volume 35, Issue 2 (2019): 77–92.
[33] Alexander Marrow and Gleb Stolyarov, 'YouTube slowdown in Russia darkens freedom of speech outlook', Reuters. 8 August 2024. YouTube was blocked by China years ago.
[34] Mylynn Felt, 'Social media and the social sciences: How researchers employ Big Data analytics', Big Data & Society Volume 3, Issue 1 (2016): 2053951716645828.
[35] Jason Gainous and Kevin M. Wagner, Tweeting to Power: The Social Media Revolution in American Politics (Oxford University Press, 2014).
[36] Yevgeniy Golovchenko, Cody Buntain, Gregory Eady, Megan A. Brown, and Joshua A. Tucker, 'Cross-platform state propaganda: Russian trolls on Twitter and YouTube during the 2016 US Presidential Election', The International Journal of Press/Politics Volume 25, Issue 3 (2020): 357–389.
[37] Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux, 2020.
[38] Paweł Golik, Arkadiusz Modzelewski, and Aleksander Jochym, 'DSHacker at CheckThat! 2024: LLMs and BERT for Check-Worthy Claims Detection with Propaganda Co-occurrence Analysis', (2024).
[39] Wendell Husebø and Matthew Boyle, 'Exclusive – Mike Johnson's top policy advisor is former lobbyist: Clients have interest in Ukraine War', Breitbart, 17 April, 2024.
[40] Dominick Mastrangelo, 'Tucker Carlson: Moscow "so much nicer than any city in my country"', The Hill, 13 February, 2024.
[41] Julia Ioffe, 'McCaul to Action', Puck, 2 April, 2024, https://puck.news/ukraine-aid-q-and-a-rep-mccaul-on-republican-support-for-bill/.
[42] Christopher Paul and Miriam Matthews, 'The Russian "firehose of falsehood" propaganda model', Rand Corporation Volume 2, Issue 7 (2016): 1–10.
[43] 'Fake news campaign targets German Army', DW. 16 February, 2017.
[44] Chris Bing and Joel Schectman, 'Special Report: How U.S. Taxpayers Funded a "Global Propaganda" Program to Push Covid-19 Vaccine Abroad', Reuters, 25 July, 2023.
[45] Claire Su-Yeon Park, Haejoong Kım, and Sangmin Lee, 'Do less teaching, do more coaching: Toward critical thinking for ethical applications of artificial intelligence', Journal of Learning and Teaching in Digital Age Volume 6, Issue 2 (2021): 97–100.
[46] Reva Schwartz, Apostol Vassilev, Kristen Greene, Lori Perine, Andrew Burt, and Patrick Hall, Towards a Standard for Identifying and Managing Bias in Aartificial Intelligence. Volume 3, US Department of Commerce, National Institute of Standards and Technology, 2022.
[47] Stephen L. Dorton and Robert A. Hall, 'Collaborative human-AI sensemaking for intelligence analysis', in International Conference on Human-Computer Interaction (Cham: Springer International Publishing, 2021), 185–201,.
[48] For more information about BERT: Mikhail V. Koroteev, 'BERT: A review of applications in natural language processing and understanding', arXiv preprint arXiv:2103.11943 (2021).
[49] Jeff Dean, 'Exciting Trends in Machine Learning', (Lecture), Rice University, Houston, TX, 13 February. 2024.
[50] Michael Bernard, George Backus, Matthew Glickman, Charles Gieseler, and Russel Waymire, 'Modeling Populations of Interest in Order to Simulate Cultural Response to Influence Activities', in Social Computing and Behavioral Modeling, 1–8.)Springer US, 2009).
[51] Seongjun Park, 'Evading, Hacking & Laundering for Nukes: North Korea's Financial Cybercrimes & the Missing Silver Bullet for Countering Them', Fordham International Law Journal Volume 45 (2021): 675.

SANANVAPAUDEN PUOLUSTAMINEN VAPAALLA VALINNALLA – KOHTI KOKO YHTEISKUNNAN KATTAVIA TEKNOLOGIAVETOISIA, IHMISKESKEISIÄ PÄÄTELAITERATKAISUJA

// Maria Papadaki

TIIVISTELMÄ: Kognitiivinen sodankäynti ja erityisesti disinformaatio nojaavat nyt voimakkaasti sosiaalisen median alustoihin, kyberteknologioihin ja tekoälyyn, tavoitteena luoda hämmennystä, yhteiskunnallista polarisaatiota, epäluottamusta, suuttumusta ja vihaa hallituksia, organisaatioita, yhteisöjä tai vastapuolen yksilöitä kohtaan. Vaikka disinformaatio on maailmanlaajuinen ongelma, sensuuriin perustuva varhainen puolustus uhkaa myös länsimaisia perusarvoja, kuten sananvapautta ja demokratiaa. Ei ole yllättävää, että kyselytutkimuksissa EU:n kansalaiset pitävät disinformaatiota uhkana demokratialle.

JOHTOPÄÄTÖKSET: Jotta voidaan tutkia puolustusvaihtoehtoja, jotka kunnioittavat demokraattisia arvoja ja ihmisoikeuksia, tarvitaan käyttäjäkeskeisiä toimintoja, jotka voivat maksimoida tuen ja minimoida inhimilliset virheet, joihin liittyy valinnanvapaus soveltaa sitä yksilötasolla.

TUTKIMUSKYSYMYS: : Miten kyberturvallisuus ja tekoäly voivat palvella demokraattisia arvoja ja ihmisoikeuksia kognitiivisten uhkien tukemisessa samalla kun pyrimme ottamaan käyttöön läpinäkyvien, mukautettavien ja kognitiivisten päätepisteiden tukityökalujen tarpeen?

JATKOTOIMENPITEET: Analysoidaan tarvetta täydentää olemassa olevaa puolustusta päätepisteissä, ja ohjeellinen toiminnallisuus hahmotellaan ja ryhmitellään eri vastetavoitteiden mukaan – eli tuen ja koulutuksen, uhkapinnan pienentämisen, havaitsemisen ja reagoinnin sekä tilannetietoisuuden mukaan. Konseptiarkkitehtuuri, vaatimusanalyysi, käyttötapaukset ja konseptin toimivuuden osoittaminen voisivat laajentaa tätä työtä havainnollistamaan sen keskeisiä kohtia.

SOSIAALISEN MEDIAN JA KANSANKIIHOTTAJIEN NOUSU

Kansankiihottajien nousu demokratian kautta ei ole uusi ilmiö, kuten eivät myöskään heidän yrityksensä hyödyntää uusia viestintävälineitä propagandan levittämiseen, kansalaisten manipulointiin ja lopulta tyranniaan. Demokratian alusta lähtien Platon on varoittanut vaarasta, että kansankiihottajat käyttävät demokratian vapauksia itseään vastaan. Nykyaikana sosiaalinen media uutena viestintävälineenä näyttää monia yhtäläisyyksiä historiallisiin esimerkkeihin, vaikkakin nyt maailmanlaajuisesti ja suuremmilla seurauksilla.

Vaikka tutkimukset ovat yhtä mieltä siitä, että valtavirran mediat, kuten sanomalehdet, radio ja televisio, ovat edelleen tärkeimmät viestintäalustat, tunnustavat ne myös sosiaalisen median kasvavan suosion uutisina ja tiedotusvälineinä, erityisesti nuorempien väestöryhmien keskuudessa. Kuten Flash Eurobarometri 536 -tutkimuksesta käy ilmi, neljännes EU:n kansalaisista, erityisesti 15–24-vuotiaista [1], on löytänyt sosiaalisesta mediasta tietoja ja tilastoja maastaan tai Euroopasta. Vastaavasti lähes kaksi viidestä vuoden 2023 Media & News -kyselyyn vastanneesta (ja kolme viidestä 15–24-vuotiaasta) käytti sosiaalista mediaa uutisten lukemiseen. [2] Prosenttiosuus oli vielä suurempi Isossa-Britanniassa, jossa lähes puolet aikuisista vastaajista ja 71 prosenttia 16–24-vuotiaista käytti sosiaalista mediaa uutisten seuraamiseen. [3] Erityisesti TikTokin nousu uutismedia-alustana on ollut jyrkkä, ja kymmenen prosenttia yli 16-vuotiaista sai uutisia sen kautta vuonna 2023, kun se vuonna 2020 oli yksi prosentti. [4]

Siksi on ymmärrettävää, että poliittiset puolueet, organisaatiot ja yksilöt käyttävät sosiaalista mediaa yleisönsä tavoittamiseen. Toisin kuin valtamediassa, jossa sama sisältö on avoimesti kaikkien sen käyttäjien saatavilla, sosiaalisen median sisältöä kuratoidaan, mikrokohdennetaan, edistetään tai tukahdutetaan näkymättömillä alusta-algoritmeilla, usein käyttäjän valinnasta riippumatta. [5] Tämä rajoittaa vastuuvelvollisuutta ja avaa oven kansankiihottajille, jotka pyrkivät käyttämään disinformaatiota manipulointiin ja polarisointiin. Auditoinnin haasteista huolimatta on syntynyt disinformaation seurantaohjelmistoja, kuten Trollrensicsin tutkijoiden kehittämä ohjelmisto. Se on löytänyt koordinoituja verkostoja, joita käytetään sosiaalisten verkostojen hukuttamiseen disinformaatiolla, kuten vuoden 2024 EU-vaalien aikana erityisesti äärioikeistolaisten puolueiden etujen vuoksi. Ranskassa, Saksassa, Italiassa ja Alankomaissa julkaistujen 2,3 miljoonan viestin analyysi paljasti 50 000 disinformaatiota levittävää tiliä. Joka viidennessä viestissä mainittiin äärioikeistolainen ranskalainen poliitikko Éric Zemmour ja joka kymmenes saksalainen Alternative für Deutschland -julkaisu tuli disinformaatiotileiltä. [6] Koska kolmen miljardin ihmisen ympäri maailmaa odotetaan äänestävän vaaleissa vuosina 2024 ja 2025, ei ehkä ole yllättävää, että Maailman talousfoorumi (WEF) on määritellyt disinformaation vakavimmaksi maailmanlaajuiseksi riskiksi seuraavien kahden vuoden aikana. WEF vahvistaa myös selkeät yhteydet disinformaation ja yhteiskunnallisen ja poliittisen polarisaation, valtioiden välisen väkivallan ja ihmisoikeuksien heikkenemisen välillä. [7] Demokratia ja ihmisoikeudet (mukaan lukien sananvapaus) ovat erityisen tärkeitä arvoja länsimaisille yhteiskunnille. [8]

DISINFORMAATIOSTA POLARISAATIOON JA KOGNITIIVISEEN SODANKÄYNTIIN

Sen lisäksi, että vaaleissa yritetään vaikuttaa itsevaltaisten ehdokkaiden hyväksi olisi tutkittava disinformaation

laajempaa roolia kognitiivisessa sodankäynnissä. Professori Miller tunnistaa disinformaation ja kehittyneet psykologiset manipulaatiotekniikat kognitiivisen sodankäynnin avainpiirteiksi. [9] Nämä tekniikat perustuvat vahvasti sosiaalisen median alustoihin, kyberteknologioihin ja tekoälyyn, ja ne ovat edelleen läheisesti yhteydessä toisiinsa sekä pyrkivät aiheuttamaan hämmennystä, yhteiskunnallista polarisaatiota, epäluottamusta, vihaa ja suuttumusta länsimaisia hallituksia, organisaatioita, yhteisöjä tai eri kantaa edustavia ihmisiä kohtaan. [10] [11] Ukrainan sota on tarjonnut runsaasti esimerkkejä disinformaation ja ulkomaisen tiedon manipuloinnin ja häirinnän (Foreign Information Manipulation & Interference, FIMI) roolista kognitiivisessa sodankäynnissä ja siitä, miten Ukrainan joukot ovat mukauttaneet puolustustaan kohtaamaan näitä. [12]

Näiden uhkien lisääntymisen salliminen voisi johtaa ääriliikkeiden, äärioikeistolaisten ja naisvihamielisten liikkeiden nousuun, mikä voisi uhata ihmisoikeuksia. Joitakin varhaisia viitteitä voidaan nähdä Lontoon King's Collegen ja Ipsosin tutkimuksessa, joka osoitti, että nuoremmat miespuoliset osallistujat ilmaisivat negatiivisempia näkemyksiä feminismistä kuin vanhemmat kollegansa. [13] Andrew Kaung, entinen TikTok-analyytikko, paljasti erot teini-ikäisten tyttöjen ja poikien saamissa sisältösuosituksissa valinnoistaan riippumatta. Teini-ikäisille pojille näytettiin väkivaltaista naisvihamielistä sisältöä; Tytöille näytettiin musiikkiin tai meikkiin liittyvää sisältöä. [14] NPCC: n lisätutkimus on osoittanut, että naisiin ja tyttöihin kohdistuvien rikosten määrä on lisääntynyt huomattavasti Yhdistyneessä kuningaskunnassa, mikä voi liittyä naisten vihaa edistävien sosiaalisen median miespuolisten vaikuttajien radikalisoitumiseen. Tuloksena on, että he ovat sittemmin päivittäneet sukupuoleen perustuvat rikokset kansalliseksi uhaksi, joka muistuttaa järjestäytynyttä rikollisuutta ja terrorismia. [15]

Esimerkki väkivaltaa ja ääriliikkeitä ruokkivasta disinformaatiosta nähtiin kolmen lapsen surman jälkeen Southportissa Isossa-Britanniassa heinäkuussa 2024. Vaikka viranomaiset julkaisivat Britanniassa syntyneen epäillyn tiedot, rikos oli jo liitetty maahanmuuttajiin ulkomaalaisomisteisten verkkosivustojen disinformaation kautta. Maahanmuuton ja väkivaltarikollisuuden välisellä väärällä yhteydellä on ollut valitettava vaikutus mobilisoimalla äärioikeistolaisia ryhmiä, jotka ovat turvautuneet hyökkäämään maahanmuuton tukirakenteita vastaan eri puolilla maata. Erityistä huomiota kiinnitettiin muslimi- ja pakolaisyhteisöihin, mikä johti yrityksiin lietsoa vihaa, väkivaltaa, ahdistusta ja pelkoa koko yhteiskunnassa. [16] [17] Olisi ennenaikaista syyttää tästä disinformaatiotapauksesta FIMIa artikkelia kirjoitettaessa. Olipa tarkoitus tai attribuutio mikä tahansa, sen vaikutukset olivat kuitenkin todellisia, ja tämä suhde olisi tunnustettava.

Euroopan Ulkosuhdehallinnon (European External Action Service, EEAS) toinen raportti FIMIn uhista tarjoaa päivitetyn katsauksen FIMI-ekosysteemiin ja paljastaa sen globaalin mittakaavan ja monipuoliset kohteet. Lähes puolet analysoiduista tapauksista kohdistui maihin ympäri maailmaa, 30 prosenttia organisaatioihin (kuten EU, Nato ja Euronews) ja lähes 20 prosenttia yksittäisiin henkilöihin, mukaan lukien ei-poliittiset henkilöt. Lisäksi sukupuoleen perustuvien ja anti-LGBTIQ sekä FIMI hyökkäykset näyttää olevan nousussa. [18]

Olisi huolimatonta olla ottamatta huomioon tekoälyn tuottaman väärennetyn sisällön mahdolliset vaikutukset, jotka WEF määritteli merkittäväksi riskiksi vuodelle 2024. [19] Huomionarvoista on, että tekoälyn tuottamaa poliitikkojen puhetta jäljittelevää ääntä on jo hyödynnetty rajoitetusti FIMI-tapauksissa. [20] Huolta aiheuttaa suhteellisen alhainen tekninen este väärennetyn sisällön luomiselle sekä nopeus ja määrä, jolla se voi tavoittaa yksilöitä. Merkittäviä esimerkkejä sen vaikutuksesta ovat

deepfake-pornografia ja pörssimanipulointi. Yhdysvaltalaisen laulajan Taylor Swiftin selkeät deepfake-kuvat keräsivät miljoonia katselukertoja ennen kuin ne lopulta poistettiin. Samoin Pentagonin räjähdyksestä kertovan deepfake-kuvan mainostaminen vaikutti Yhdysvaltain osakemarkkinoihin ennen kuin Yhdysvaltain viranomaiset torjuivat huhut. [21]

On mahdollista, että tämä pelottelun, polarisaation ja väkivallan ilmapiiri, jossa FIMI on esillä, johtaa myös itsesensuuriin, apatiaan tai pakottamiseen, jos ihmiset pelkäävät puhumisesta seuraavia ei toivottuja kunnianloukkauksia tai väkivaltaa. Vuoden 2023 Freedom of the Net -raportti osoittaa, että sananvapautta vastaan on hyökätty huomattavan paljon. [22] Kolmessa neljäsosassa tutkituista maista yksityishenkilöille on aiheutunut oikeudellisia seuraamuksia siitä, että he ovat ilmaisseet itseään verkossa. Neljässä seitsemästä maasta tämä on johtanut jopa fyysiseen väkivaltaan tai ihmishenkien menetykseen.

SENSUURI VS. VAPAA VALINTA

Autokraattisten hallintojen tiedetään turvautuvan tavanomaiseen ja tekoälyyn perustuvaan sensuuriin oman narratiivin hallitsemiseksi. Tämä voi ilmetä monin tavoin, mukaan lukien eriävän poliittisen, uskonnollisen tai sosiaalisen sisällön estämisenä, sananvapauden tukahduttamisena ja asteittaisena mutta johdonmukaisena poikkeamana kansainvälisistä ihmisoikeussopimuksista. [23] Sensuuri ei kuitenkaan voi toimia länsimaisissa yhteiskunnissa loukkaamatta lopulta niiden perusarvoja ja vapauksia. WEF tuo esiin riskin, että jotkut hallitukset toimivat liian hitaasti, kun otetaan huomioon kompromissi disinformaation estämisen ja sananvapauden suojelemisen välillä. Samaan aikaan toiset voivat heikentää ihmisoikeuksia ja lisätä sensuuria omaksumalla autoritaarisia käytäntöjä. [24]

Myös EU:n kansalaiset tunnistavat nämä riskit ja pitävät disinformaatiota isoimpana uhkana demokratialle. [25] Kognitiivisen sodankäynnin syvemmän ymmärtämisen ja yhteistyöhön perustuvan monitasoisen puolustuksen kehittämiseksi on käynnissä huomattavaa työtä. [26] [27] Huomionarvoinen ja kattava viitekehys FIMIn uhkiin vastaamiseksi on FIMI-työkalupakki, joka perustuu monitasoiseen, yhteistyöhön perustuvaan, monitieteiseen ja koko yhteiskunnan kattavaan lähestymistapaan. [28]

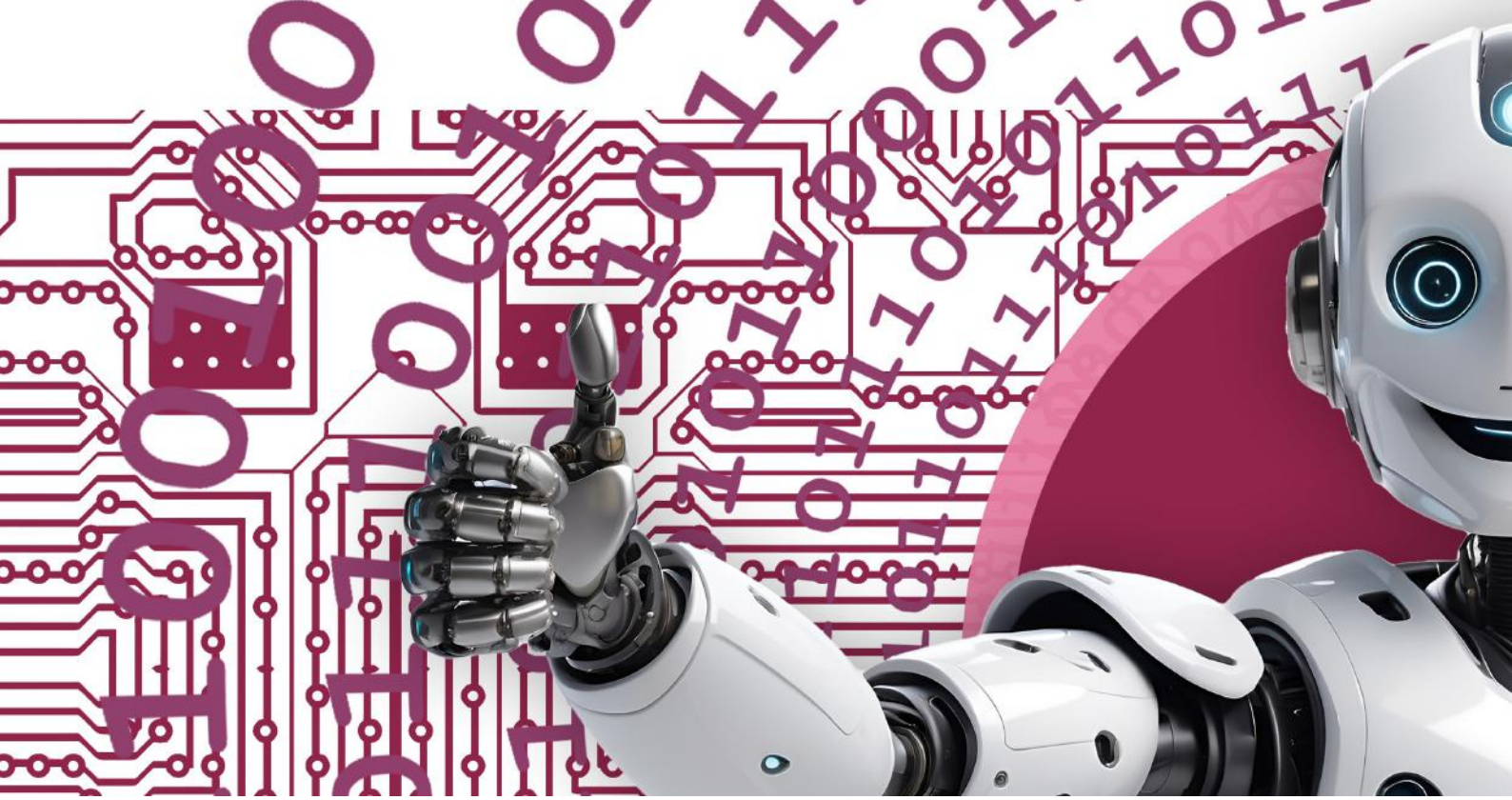
Kun pohditaan, kenellä on oikeus ja vastuu päättää suojan tasosta, on useita sidosryhmiä, joilla kaikilla on omat vastuunsa. Vaikka viranomaisilla on valtuudet määritellä, säännellä ja estää laittoman toiminnan malleja, on vielä tilaa lisäsuojelulle, josta yksittäiset kansalaiset voivat olla vastuussa, jos he päättävät tehdä niin.

KÄYTTÄJIEN ALTTIUS VALETARINOILLE

Maertens kumppaneineen suunnitteli väärän tiedon herkkyystestin (MIST) ymmärtääkseen inhimillisten virheiden laajuuden väärennettyjen tarinoiden tunnistamisessa. [29] Noin 1 500 Yhdysvaltain kansalaiselle tehdyssä tutkimuksessa havaittiin, että kaksi kolmesta uutisesta voitiin tunnistaa oikein. Nuoremmat aikuiset ja ne, jotka luottivat sosiaaliseen mediaan uutisissaan, menestyivät kuitenkin huonommin. [30] Samaan aikaan EU:ssa tehty Eurobarometri-tutkimus osoitti, että 30 prosenttia kyselyyn vastanneista EU:n kansalaisista ei luottanut tunnistavansa disinformaatiota. Luottamus heikkeni iän myötä ja kasvoi koulutustason myötä. [31] Yhdistyneessä kuningaskunnassa toimivan Ofcomin tutkimus raportoi vastaavasta epävarmuudesta, jossa joka kolmannen internetin käyttäjän Yhdistyneessä kuningaskunnassa todettiin olevan epävarma tai tietämätön verkossa olevien tietojen totuudenmukaisuudesta. Huomionarvoista on myös se, että pieni osajoukko, kuusi prosenttia, jopa uskoi kaiken verkossa olevan kiistatta totta. [32] Voidaan sanoa, että virheiden tai epävarmuuden tasot ovat korkeat, erityisesti kun otetaan huomioon toiseen ihmiseen liittyvän uhan, tietojenkalastelun, virhetasot. Vaikka vuoden 2024 Verizon Data Breach Investigations -raportti ei ole suoraan vertailukelpoinen, se voi silti olla harkitsemisen arvoinen. Se viittaa siihen, että tietojenkalasteluviestien avaamisen todennäköisyydet vaihtelivat kolmesta kymmeneen prosenttiin viimeisten kahdeksan vuoden aikana. [33]

Virhetasojen vähentämiseksi voi olla hyödyllistä tarkastella koulutuksen mahdollisia vaikutuksia. Tietojenkalastelun tapauksessa Spitzner ehdottaa empiirisesti, että ensimmäiset kalasteluviestien avaamisen tilastot organisaation tietoisuuden lisäämisen alussa voivat tyypillisesti vaihdella 25–30 prosentin välillä, ennen kuin ne lopulta laskevat alle viiteen 18–22 kuukauden kuluessa. [34] Tietoisuus ja koulutus voivat korostaa kognitiivisia vinoumia ja emotionaalista manipulointia ja kannustaa kriittiseen ajatteluun, jolloin ihmiset voivat havaita varoitusmerkkejä epätavallisista ja odottamattomista hyökkäyksistä. On myös syytä tunnustaa laajempi valikoima täydentäviä monikerroksisia teknologisia lähestymistapoja, jotka voivat auttaa vähentämään uhkatilaa automaation avulla ja viime kädessä inhimillisten virheiden todennäköisyyttä kannustamalla käyttäjiä noudattamaan turvallisuusnormeja. Näitä voivat olla sähköpostin sisällön suodatus, tunnettujen tilien mustalle listalle lisääminen, sähköpostin alkuperän todennus ja vahvistus (DMARC:n, DKIM:n ja SPF:n muodossa).

Palataksemme FIMIin ja disinformaatioon, olisi hyödyllistä pohtia, miten tekoäly ja ihmiskeskeinen turvallisuus voisivat auttaa vähentämään inhimillisten virheiden todennäköisyyttä (olettaen, että käyttäjän



suostumus on olemassa). Tähän voi sisältyä uhkatilan vähentäminen, tarinoiden legitiimiyden tai aitouden erottamisen kognitiivinen kuormitus sekä ihmisten ja teknologisten kontrollien välinen teknologinen kuilu.

DISINFORMAATION HAVAITSEMINEN

Alustavana askeleena inhimillisten virheiden vähentämiseksi ja käyttäjätuen maksimoimiseksi tässä osiossa tarkastellaan disinformaation havaitsemisen lähestymistapoja, mukaan lukien asenneanalyysi, leviämismallien analyysi, alkuperän maine, alkuperä, syvähuijaustunnistus, vahvistusharhan käyttäjäprofilointi ja faktantarkistus. Tyhjentävän luettelon sijaan tämä edustaa valikoimaa lähestymistapoja, jotka ovat vaikuttaneet tässä artikkelissa esitettyihin vaihtoehtoihin.

Varhaiset lähestymistavat keskittyivät merkkeihin emotionaalisesti latautuneesta manipuloivasta kielestä tai diskurssimalleista, jotka esiintyivät uutisissa ja sosiaalisen median reaktioissa. Nämä lähestymistavat sisälsivät luonnollisen kielen käsittelyä ja sosiaalisen verkoston sisällön asenneanalyysiä, erityisesti X/Twitterissä. [35]

Huomionarvoinen ja merkittävä indikaattori on se, miten nämä tarinat leviävät. Tutkimukset osoittivat, että voimakkaiden reaktioiden herättämiseen tähtäävät tarinat levisivät todennäköisesti nopeammin tai ainakin eri tavalla kuin aidot uutiset. Toinen epänormaalien etenemismallien tunnistamisen etu on, että se on sisältöagnostinen, mikä tekee siitä helpommin sovellettavissa monikielisiin ympäristöihin. Graafiset neuroverkot tai ajalliset kaavioverkot voivat olla erityisen tehokkaita osoittamaan merkkejä nopeasti kasvavista uutisista, jopa sopeutumaan kehittyviin leviämismalleihin. [36] [37]

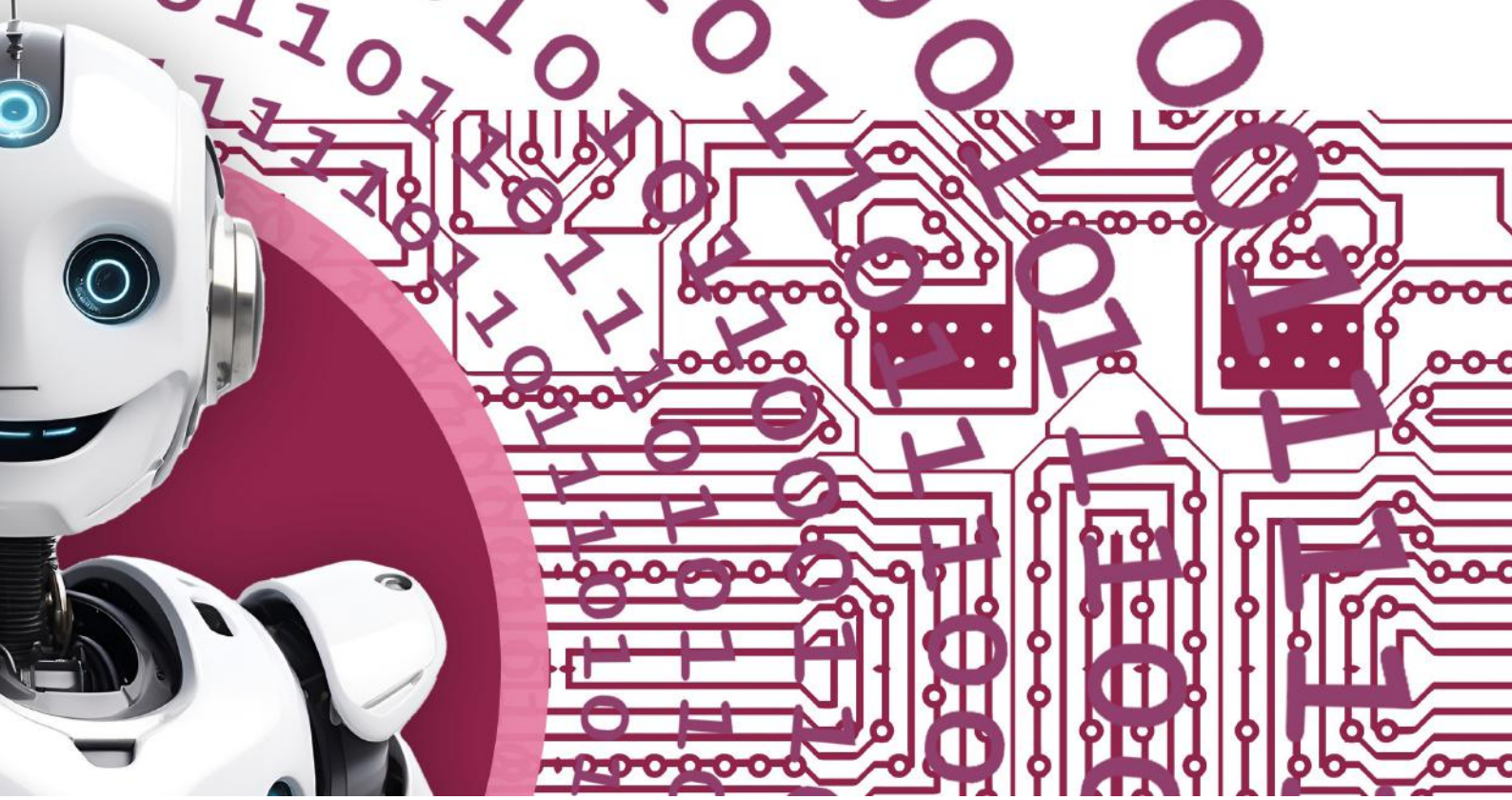
Samoin voi olla mahdollista tunnistaa disinformaatiota levittävien bottitilien poikkeava käyttäytyminen maineensa tiedostamisen perustaksi. Aloitteet, kuten Coalition for Content Provenance and Authenticity (C2PA), voisivat mennä vielä pidemmälle allekirjoittamalla mediasisällön kryptografisesti sen lähteen ja muokkaushistorian tarkistamiseksi. Alkuperätietojen olemassaolo tai jopa niiden puuttuminen voisi auttaa parantamaan luottamusta kuva-, ääni- tai videosisällön aitouteen ja alkuperään. [38]

Syvähuijaustunnistuksen tarkoituksena on tunnistaa tekoälyn luomien ohjelmistojen muokkausprosessien aiheuttamat poikkeavat vaikutukset. Syvähuijausvideoissa tällaisia epäjohdonmukaisuuksia voidaan havaita keskeisten kasvopisteiden liikkeessä tai kohdistusvirheissä, epätavallisessa valaistuksessa, varjoissa ja heijastuksissa sekä yksittäisissä kehyksissä että jaksoissa. Syväväärennösten havaitsemiseen voidaan käyttää erilaisia menetelmiä, ja syväoppiminen ja multimodaaliset syväoppimisen lähestymistavat osoittautuvat erityisen tehokkaiksi. [39]

Yksi indikaattori ottaa huomioon mahdollisuuden, että henkilö todennäköisemmin uskoo ja levittää väärää tietoa, jos se on jo linjassa heidän olemassa olevien uskomustensa kanssa, ilmiö, joka tunnetaan nimellä vahvistusharha. Käyttäjien käyttäytymisprofiilit niiden aiemmasta käytöstä voisivat siten auttaa ennustamaan henkilöitä, jotka voivat tahattomasti levittää väärää tietoa. [40]

Edellä mainitut tekniikat on suunniteltu havaitsemaan eri yksiköiden erilaisia poikkeavan toiminnan malleja, mikä voi osoittaa, että disinformaation havaitseminen on todella mahdollista. Näitä tekniikoita voidaan edelleen parantaa yhdistämällä niitä tai jopa täydentämällä niitä kartoittamalla FIMIn ja kyberpoikkeamien laajempia piirteitä, sellaisina kuin ne on määritelty DISARM- ja ATT&CK-kehyksissä. [41]

Lopuksi on tärkeää pohtia tietokoneen ja ihmisen välisten yhteistyömenetelmien suurta potentiaalia



faktantarkistuksen yhteydessä. Yhteisöt ympäri maailmaa tekevät yhteistyötä tutkiakseen journalistisiin standardeihin perustuvan tiedon paikkansapitävyyttä ja purkaakseen disinformaation taustalla olevan narratiivin, aikomuksen ja mahdollisen vaikutuksen. [42] Disinformaatiotietojoukoilla koulutettujen suurten kielimallien (LLM) ja generatiivisen tekoälyn nouseva ala sisältää faktantarkistustoiminnon. Ne ovat tärkeitä ja erityisen merkityksellisiä myös loppukäyttäjille. Vaikka LLM: t vaikuttavat lupaavilta, olisi järkevää odottaa lisätodisteita niiden tarkkuudesta ja kestävyydestä disinformaatiohyökkäyksiä vastaan.

KOHTI PÄÄTELAITERATKAISUJA FIMI-UHKIIN VASTATESSA

Vaikka kyberturvallisuuden periaatteet ovat innoittaneet FIMIn työkalupakkia, on tärkeää tunnustaa sen vahvemmat sosiokognitiiviset elementit, jotka ulottuvat teknisiä näkökohtia pidemmälle kattamaan laajemman valikoiman yhteiskunnallisia näkökohtia. Sen kollektiivisen reagoinnin protokolliin kuuluu laaja asiaankuuluvien sidosryhmien verkosto koko yhteiskunnassa, joista jokaisella on erilliset vastuut, mikä varmistaa oikeasuhteiset, mukautuvat, kollektiiviset, ymmärrettävät ja tehokkaat vastaukset. [43]

Käyttäjillä ja kansalaisilla on sidosryhminä rooli ja vastuu suojella tietotilaansa ja tutkia, miten vastausmalli voitaisiin tarjota avoimesti ja demokraattisesti. Tätä varten ehdotetaan, että suojaus-, tunnistus- ja tukitoiminnot ovat käytettävissä päätepisteissä, joissa käyttäjät voivat vapaasti päättää, mitkä he ottavat käyttöön mukautettavien oletusasetusten tuella. Tällainen käyttäjäkeskeinen toiminnallisuus tarjoaisi mahdollisuuden mahdollisimman suureen tukeen, minimoisi inhimillisten virheiden riskin ja antaisi jokaiselle vaihtoehdolle mahdollisuuden ottaa se käyttöön tai poistaa se käytöstä käyttäjätasolla. Seuraavassa esitetään joukko ohjeellisia vaihtoehtoja käyttäjille: tuki ja koulutus; uhkapinnan vähentäminen; havaitseminen ja reagointi; sekä tilannetietoisuus.

TUKI JA KOULUTUS

Käyttäjien aloittama tuki, joka helpottaa faktantarkistuksen, uskottavuuden/maineen pisteytyksen, bottien havaitsemisen, disinformaation seurannan ja koulutuksen käyttöä, voidaan tarjota käyttäjille selainlaajennusten, kontekstivalikkovaihtoehtojen tai LLM:ien kautta. Esimerkiksi deepfake-äänen ja -videon varmennustoimintoa (joka muistuttaa Microsoft Video Authenticatorin, Like AI:n, Sensity AI:n tai WeVerifyn kaltaisia ratkaisuja) voidaan käyttää deepfake-äänen tai -videoiden uskottavuuden tarkistamiseksi. Yksinkertaistetut raportit faktantarkistusta, käänteisiä kuvahakuja ja sisällön tarkistamista varten voivat myös osoittautua hyödyllisiksi. Lisäksi voitaisiin helpottaa koulutusresurssien saatavuutta, jotta käyttäjät tunnistaisivat disinformaation ja emotionaalisen manipuloinnin varoitusmerkit, käyttäisivät sopivia välineitä, ymmärtäisivät niiden tuloksia ja valitsisivat sopivat ja oikeasuhteiset reagointivaihtoehdot. Tukitoiminto voisi myös helpottaa disinformaatioresurssien ja -yhteisöjen saatavuutta käyttäjille, jotka haluavat tehdä vapaaehtoistyötä, olla yhteydessä toisiinsa tai ilmoittaa epäillyistä uhista. [44]

UHKAPINNAN PIENENTÄMINEN

Vaihtoehtoja uhkapinnan pienentämiseksi voisivat olla automaattiset vastatoimet tunnetuille uhille, joita käyttäjät eivät halua kohdata säännöllisesti. Useita vastatoimia voidaan käyttää, kuten merkityn sisällön korostaminen,

suodattaminen, korvaaminen aidolla vaihtoehdolla tai tallentaminen toissijaiseen vaihtoehtoon tulevaa tarkistusta varten (samanlainen kuin roskapostikansiot epäillylle roskapostille). Oletusasetus voidaan esimerkiksi määrittää suodattamaan automaattisesti tunnettuihin disinformaatiotileihin liittyvää sisältöä. Käyttäjä voi kuitenkin myös suodattaa pois poliittisen syvähuijaussisällön tai väkivaltaa ja ääriajattelua koskevan sisällön. Toinen käyttäjä saattaa haluta ohjata poliittisen sisällön, jolla ei ole vahvistettua alkuperää, toissijaiseen sijaintiin myöhempää tarkistusta varten. Tarpeettomien teknologisten esteiden välttämiseksi olisi hyödyllistä mukauttaa suositeltuja oletusasetuksia ja käyttäjäystävällisiä käyttöliittymiä, jotka kannustavat oikeasuhteiseen ja asianmukaiseen uhkien vähentämiseen käytetyistä sosiaalisen median sovelluksista riippumatta.

HAVAITSEMINEN JA REAGOINTI

Havaitsemistoiminnossa voitaisiin keskittyä jäännösaktiivisuuden tunnistamiseen ja hienovaraisempien varoitusmerkkien tunnistamiseen uusista disinformaatiouhista. Tällaiset tapaukset voidaan ilmoittaa käyttäjälle, eskaloida ihmisen ja tietokoneen tiimeille analysointia varten tai kirjata paikallisesti tulevaa tutkimusta varten. Voi esimerkiksi olla mahdollista tunnistaa käyttäjät, jotka ovat alttiita tahattomasti välittämään väärää tietoa muille. Käyttäjän toimintaraportti, jossa korostetaan vääriä tietoja, voi johtaa hyödyllisiin kehotteisiin ja ohjeisiin asiaankuuluvaan opetussisältöön.

TILANNEKUVA

Voi olla hyödyllistä vaihtaa uhkatiedustelutietoja, jotka auttavat tilannetietoisuutta ja auttavat yhdistämään tapahtumia muihin aloihin. Tapahtuman jälkeinen käyttäjäasetusten tarkistus voi myös kuulua tähän toimintoryhmään.

JOHTOPÄÄTÖKSET JA TULEVA TYÖSKENTELY

Merkittävä huoli disinformaatiosta, demokraattisten arvojen merkitys ja käyttäjien ilmaisema epävarmuus kyvystään tunnistaa disinformaatio oikein viittaavat tarpeeseen vahvistaa suojaa päätepisteissä ja osoittavat, että käyttäjät saattavat olla halukkaita ottamaan käyttöön ehdotetut toiminnot. Teknologinen kuilu tai yksityisyyden suojaan liittyvät huolenaiheet voivat osoittautua esteiksi joillekin ihmisille. Generatiivinen tekoäly voi osoittautua erityisen hyödylliseksi käyttäjätuen teknisten aukkojen paikkaamisessa, samoin kuin optimaalisten oletusprofiiliasetusten käyttö. Tietoisuuden lisääminen yksityisyyttä parantavista tekniikoista voisi lievittää pelkoja ja parantaa yksityisyyden suojaa.

Yksityisyyttä parantavat teknologiat, kuten eriytetty yksityisyys ja yhdistetty oppiminen, voisivat mahdollistaa asiaankuuluvien tietojen hyödyllisyyden ja samalla varmistaa niiden yksityisyyden tietosuojaperiaatteiden mukaisesti. Tämä on erityisen tärkeää havaitsemisen ja reagoinnin, tilannetietoisuuden tai käyttäjäprofiloinnin tukemiseksi, kun yksityisyyden suojaa koskevat vaatimukset olisivat korkeammat. Koska painopiste on sisällön tutkimisessa eikä käyttäjien käyttäytymisessä, voidaan väittää, että tuen, koulutuksen ja uhkatilan vähentämistoiminnon tietosuojavaatimukset olisivat suhteellisesti alhaisemmat. Päätepistetoimintojen tietosuojavaatimukset on joka tapauksessa määritettävä ja perusteltava ennen käyttäjän suostumuksen pyytämistä.

Ehdotetun päätepistetoiminnon tarkoituksena on täydentää olemassa olevia suojauksia ja sosiaalisen median valvontaa demokratisoimalla suojausta. Sillä pyritään antamaan käyttäjille oikeus ja velvollisuus hallita omaa tietotilaansa sosiaalisen median sovelluksista riippumatta, mikä edistää avoimuutta. Sen tavoitteena on kuroa umpeen teknologinen kuilu ihmisten ja disinformaation torjunnan välillä, maksimoida tuki, vähentää inhimillisten virheiden todennäköisyyttä ja edistää turvallista käyttäytymistä normina. Se pyrkii myös tarjoamaan yksilöille valinnanvapautta tapauksissa, joissa keskitetty valvonta voisi heikentää demokraattisia arvoja ja ihmisoikeuksia. Konseptiarkkitehtuuri, vaatimusanalyysi, käyttötapaukset ja konseptin toimivuuden todistaminen voisivat laajentaa tätä työtä tulevaisuudessa havainnollistamaan sen keskeisiä kohtia. ■

MARIA PAPADAKI

Tohtori Maria Papadaki on kyberturvallisuuden apulaisprofessori Derbyn yliopistossa, Isossa-Britanniassa. Hänen tutkimusintressinsä keskittyvät häiriötilanteisiin reagointiin, uhkatiedusteluun, merenkulun kyberturvallisuuteen ja ihmiskeskeiseen turvallisuuteen. Hänen tuotantoonsa kuuluu yli 70 kansainvälistä vertaisarvioitua julkaisua tällä alalla. Tämän artikkelin sisältämät näkemykset ovat kirjoittajan omia näkemyksiä, eivätkä edusta Derbyn yliopiston yleisiä näkemyksiä.

LÄHTEET:

[1] European Commission, 'Flash Eurobarometer 536 Report: Public awareness and trust in European statistics', February 2024, https://europa.eu/eurobarometer/surveys/detail/2955.

[2] European Parliament, 'Media & News Survey 2023', November 2023, https://europa.eu/eurobarometer/surveys/detail/3153.

[3] OFCOM, 'News consumption in the UK: 2023, Research findings', July 2023, https://www.ofcom.org.uk/media-use-and-attitudes/attitudes-to-news/news-consumption/.

[4] Idem.

[5] Urbano Reviglio and Claudio Agosti, 'Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media', Social Media + Society Volume 6 Issue 2 (April 2020), https://doi.org/10.1177/2056305120915613.

[6] Lisa O'Carroll, 'Disinformation networks "flooded" X before EU elections, report says', July 2024, https://www.theguardian.com/world/article/2024/jul/12/disinformation-networks-social-media-x-france-germany-italy-eu-elections.

[7] World Economic Forum, 'The Global Risks Report 2023: 18th Edition Insight Report', January 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[8] European Parliament, 'Eurobarometer: Parlemeter 2022', January 2023, European Commission, 'Flash Eurobarometer 536 Report: Public awareness and trust in European statistics', February 2024, https://europa.eu/eurobarometer/surveys/detail/2955.

[9] Seumas Miller, 'Cognitive warfare: An ethical analysis', Ethics and Information Technology Volume 25, Issue 46 (September 2023), https://doi.org/10.1007/s10676-023-09717-7.

[10] Nicolas Hénin, 'FIMI: Towards a European redefinition of Foreign Interference', EU Disinfo Lab, April 2023, https://www.disinfo.eu/publications/fimi-towards-a-european-redefinition-of-foreign-interference/.

[11] Erika Magonara and Apostolos Malatras, 'Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape', ENISA, December 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape/.

[12] Jakub Kalenský and Roman Osadchuk, 'How Ukraine fights Russian disinformation: Beehive vs mammoth', Hybrid CoE Research Report 11, January 2024.

[13] King's College London and Ipsos, 'Emerging tensions? How younger generations are dividing on masculinity and gender equality', February 2024, https://www.kcl.ac.uk/policy-institute/assets/emerging-tensions.pdf.

[14] Marianna Spring, '"It stains your brain": How social media algorithms show violence to boys', BBC Panorama, September 2024, https://www.bbc.co.uk/news/articles/c4gdqzxypdzo.

[15] NPCC, 'Violence Against Women and Girls (VAWG): National Policing Statement 2024', July 2024, https://cdn.prgloo.com/media/5fc31202dd7e411ba40d29fdca7836fd.pdf.

[16] Mark Easton, 'Protests reveal deep-rooted anger, but UK is not at boiling point', August 2024, https://www.bbc.co.uk/news/articles/czx66dkx3wlo.

[17] Marianna Spring, 'Did social media fan the flames of riot in Southport?', July 2024, https://www.bbc.co.uk/news/articles/cd1e8d7llg9o.

[18] European External Action Service (EEAS), '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence', January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[19] World Economic Forum, 'The Global Risks Report 2023: 18th Edition Insight Report', January 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[20] European External Action Service (EEAS), '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence', January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[21] Luke Hurst, 'How a fake image of a Pentagon explosion shared on Twitter caused a real dip on Wall Street', Euronews, May 2023, https://www.euronews.com/next/2023/05/23/fake-news-about-an-explosion-at-the-pentagon-spreads-on-verified-accounts-on-twitter.

[22] Shahbaz, Funk, and Vesteinsson, 'The Repressive Power of Artificial Intelligence', in Freedom on the Net 2023, Shahbaz, Funk, Vesteinsson, Brody, Baker, Grothe, Barak, Masinsin, Modi, and Sutterlin, eds (Freedom House, 2023), freedomonthenet.org.

[23] Idem.

[24] World Economic Forum, 'The Global Risks Report 2023: 18th Edition Insight Report', January 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[25] European Commission, 'Flash Eurobarometer 464: Fake news and disinformation online', April 2018, https://europa.eu/eurobarometer/surveys/detail/2183.

[26] European External Action Service (EEAS), '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence', January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[27] European External Action Service (EEAS), '1st EEAS Report on Foreign Information Manipulation and Interference Threats towards a framework for networked defence', February 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf.

[28] European External Action Service (EEAS), '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence', January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[29] Rakoen Maertens, Friedrich M. Götz, Hudson F. Golino, Jon Roozenbeek, Claudia R. Schneider, Yara Kyrychenko, John R. Kerr, Stefan Stieger, William P. McClanahan, Karly Drabot, James He, and Sander van der Linden, 2024, 'The Misinformation Susceptibility Test (MIST): A psychometrically validated measure of news veracity discernment', Behaviour Research Methods Volume 56, 1863–1899 (March 2024), https://doi.org/10.3758/s13428-023-02124-2.

[30] Linley Sanders, 'How well can Americans distinguish real news headlines from fake ones?', June 2023, https://today.yougov.com/politics/articles/45855-americans-distinguish-real-fake-news-headline-poll.

[31] European Parliament, 'Media & News Survey 2022', July 2022, https://europa.eu/eurobarometer/surveys/detail/2832.

[32] OFCOM, 'The genuine article? One in three internet users fail to question misinformation', March 2023, https://www.ofcom.org.uk/media-use-and-attitudes/attitudes-to-news/one-in-three-internet-users-fail-to-question-misinformation/.

[33] Verizon, '2024 Data Breach Investigations Report', May 2024, https://www.verizon.com/business/resources/reports/dbir/.

[34] Lance Spitzner, 'Why a Phishing Click Rate of 0% is Bad', November 2017, https://www.sans.org/blog/why-a-phishing-click-rate-of-0-is-bad/.

[35] Shreya Ghosh and Mitra Prasenjit, 2023.'"Review of How Early Can We Detect? Detecting Misinformation on Social Media Using User Profiling and Network Characteristics', in Lecture Notes in Computer Science, Gianmarco De Francisci Morales, Claudia Perlich, Natali Ruchansky, Nicolas Kourtellis, Elena Baralis, and Francesco Bonchi, eds, Vol. 14174, Springer. https://doi.org/10.1007/978-3-031-43427-3_11.

[36] Idem.

[37] Frederico Monti, Fabrizio Frasca, Davide Eynard, Damon Mannion, and Michael M. Bronstein, 'Review of Fake News Detection on Social Media Using Geometric Deep Learning', in: Representation Learning on Graphs and Manifolds Workshop, ICLR 2019, May 2019, Ernest N. Morial Convention Center, New Orleans, USA, https://rlgm.github.io/papers/34.pdf.

[38] Microsoft, 2023, 'Microsoft Digital Defense Report: Building and improving cyber resilience', October 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[39] Md Shohel Rana, Mohammad Nur Nobi, Beddhu Murali, and Andrew H. Sung, 'Deepfake Detection: A Systematic Literature Review', in IEEE Access, Volume 10, 25494–25513, 2022, doi: 10.1109/ACCESS.2022.3154404.

[40] Yingtong Dou, Kai Shu, Congying Xia, Philip S. Yu, and Lichao Sun, 2021, July, User preference-aware fake news detection, in Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval (2051–2055).

[41] 'DISARM Framework Explorer', DISARM Frameworks, last modified November 2023, https://disarmframework.herokuapp.com/.

[42] EU Disinfo Lab, 'Tools to monitor disinformation', 2024, https://www.disinfo.eu/resources/tools-to-monitor-disinformation/.

[43] European External Action Service (EEAS), '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence', January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[44] EU Disinfo Lab, 'Tools to monitor disinformation', 2024, https://www.disinfo.eu/resources/tools-to-monitor-disinformation/.

TAISTELEMMEKO VARJOSSA?

// Matthias Wasinger

TIIVISTELMÄ: Eksistentiaalisten uhkien tunnistaminen on ratkaisevan tärkeää tappion välttämiseksi. Tällaisen uhkan muodostaa esimerkiksi kognitiivinen sodankäynti. Asevoimien sopeutumiskyvyn hyödyntäminen toimii länsimaisille yhteiskunnille yhtenä keinona vastata tällaisiin uhkiin. Pelkästään armeijaan luottaminen aiheuttaa kuitenkin riskejä, joten tarpeen on edellyttää kokonaisvaltaista lähestymistapaa kansalliseen turvallisuuteen. Kaikkien demokraattisessa valvonnassa olevien keinojen koordinointi on olennaista tehokkaiden tulosten saavuttamiseksi. Länsimaisten asevoimien tulisi keskittyä pelotteeseen ja tukea poliittista päätöksentekoa. Siviileihin kohdistuva kognitiivinen sodankäynti edellyttää jatkuvaa yhteiskunnallista koulutusta ja parempaa viestintää hallituksilta. Vaikka kansainvälinen oikeus käsittelee erilaisia haasteita, kognitiivisen sodankäynnin aiheuttamiin haasteisiin ei välttämättä ole oikeudellista ratkaisua. Nykyaikaisten uhkien edessä Euroopan on puolustettava arvojaan kattavin, koordinoiduin ja synkronoiduin keinoin.

JOHTOPÄÄTÖKSET: Sotia käydään usein muilla välineillä kuin sotilaallisella voimalla. Armeija voi kuitenkin tukea uhkaan vastaamista. Kovien keinojen lisäksi armeijat voivat tarjota poliittiselle johdolle arvokkaita neuvoja, menettelytapoja ja tekniikoita, joiden avulla hallitukset voivat torjua eksistentiaalisia uhkia.

TUTKIMUSKYSYMYS: Kuinka sotilasvoimaa voidaan käyttää kognitiivisen sodankäynnin torjumiseen?

JATKOTOIMENPITEET: Nykyaikaisella valtiolla on käytössään enemmän kuin vain yksi vallan väline. Koordinoituina ja synkronoituina näillä välineillä voidaan saavuttaa tehokkaimmat ja vaikuttavimmat tulokset neuvotteluissa. Armeijan roolin osana työkalupakkia pitäisi olla kaksijakoinen. Sen on varmistettava uskottava pelote ja tarjottava samalla arvokkaita prosesseja, menettelytapoja ja tekniikoita.

EPÄREILU PELI; KAKSI LÄHESTYMISTAPAA

Herodotoksen mukaan persialaisten uhatessa kreikkalaisia niin monilla nuolilla, että ne peittivät auringon Thermopylaen taistelun aikana vuonna 480 eaa., spartalainen soturi Dienekes vastasi: "Sitten taistelemme varjossa". [1] Seuraavina vuosisatoina useat valtiomiehet ja filosofit ovat siteeranneet ja tulkinneet uudelleen tätä lainausta. Sen alkuperäinen merkitys on kehittynyt. Alkuperäinen lausunto korosti paradoksaalisesti edullista vaikutusta taistelemalla varjossa paahtavan auringon sijaan. [2] Toinen mahdollinen tulkinta kehittyi kuitenkin vuosisatojen aikana: tämä oli kärsivällisyys ylivoimaisen uhan edessä. [3] Eksistentiaalisen uhan edessä muinainen Kreikka, eurooppalaisen kulttuurin kehto, loi puitteet sodan voittamiselle etsimällä etua alemmuudesta tai uhmakkaasta vastarinnasta.

Yli kaksituhatta vuotta myöhemmin Eurooppa on jälleen eksistentiaalisen uhan edessä. Venäjän hyökkäys Ukrainaan ei ole pelkkä valtioiden välinen konflikti mantereen itäreunalla. Se on osa tavoitetta, jolla pyritään hävittämään länsimainen elämäntapa, tunnustettu kansainvälinen oikeudellinen kehys, eurooppalaiset arvot ja ylikansallinen yhteenkuuluvuus. [4] Tätä varten Venäjä ja sen kumppanit ovat pitkään käyneet hybridisotaa Eurooppaa vastaan. Toisin kuin persialaisissodissa, aseet eivät ole enää nuolia. Disinformaatiokampanjat, informaatiosodankäynti ja kognitiivinen sodankäynti heikentävät yhteenkuuluvuuden tunnetta, ylikansallista solidaarisuutta ja kansalaisten tukea ulkoisen uhan torjumiselle. [5] Nämä keinot jäävät selvästi aseellisen konfliktin kynnyksen alapuolelle, mutta haastavat silti länsimaisia yhteiskuntia. [6] Kun uhka on tunnistettu ja tunnustettu, Eurooppa voi kuitenkin päättää, miten taistella vastaan, löytämällä edun sekasorrosta ja olemalla uhmakkaasti kärsivällinen.

EI VASTAUSTA ILMAN TUNNUSTUSTA

Kaikkiin uhkiin vastaamisen kulmakivi on niiden julkinen poliittinen tunnustaminen. Erityisesti Euroopalta puuttuu kuitenkin edelleen yhteinen tilannetietoisuus. Venäjän sotilaallisia tunkeutumisia Georgiaan vuonna 2008 ja Ukrainaan vuonna 2014 ei seurannut kansainvälinen tuomitseminen tai eristäminen. [7] Päinvastoin, myönnytyspolitiikka ja taloudellisen riippuvuuden syventäminen, erityisesti fossiilisen energian suhteen, johtivat yleiseen tietämättömyyteen tuskallisesta tosiasiasta: Venäjän itsevarmuus ei enää rajoittunut diplomatian saralle. Edes Venäjän hallituksen räikeitä – ja valitettavasti onnistuneita – yrityksiä "palkata" entisiä korkea-arvoisia eurooppalaisia poliitikkoja, kuten Saksan entinen liittokansleri Gerhard Schröder ja Ranskan entinen pääministeri François Fillon, ei otettu vakavasti. [8] Edes Venäjän viimeisintä hyökkäystä Ukrainaan ei vieläkään tunnusteta sellaisena kuin se on: suorana hyökkäyksenä kansainvälistä lakia ja järjestystä sekä eurooppalaisia arvoja vastaan.

Ukrainassa käynnissä oleva kulutussota on vain ilmeisin oire Venäjän aggressiosta. Tämän julman ja näkyvän sodan alla Venäjä ja sen kumppanit käyvät piilotellumpaa sotaa länttä vastaan. Tämä on sota herruudesta informaation alalla, taistelu paremmuudesta tiedon jakamisessa ja tulkinnassa. [9] Tavoitteena on muokata ja vaikuttaa siihen, mitä yhteiskunnat ajattelevat ja ymmärtävät menneistä, meneillään olevista ja tulevista tapahtumista, sekä vähentää - ellei tuhota - länsimaisten yhteiskuntien luottamusta ja uskoa arvoihin ja halukkuutta puolustaa niitä. [10]

Vaikka länsimaisten yhteiskuntien tuki Ukrainalle on merkittävää ja on epäilemättä mahdollistanut sen Venäjän aggressiolta puolustautumisen tähän mennessä,[11] voidaan kysyä, tunnustetaanko ongelma kokonaisuudessaan uhaksi paitsi Euroopan itäreunalla sijaitsevalle maalle myös hyökkäykseksi demokraattisia arvoja vastaan. Samaan aikaan kun varoja virtaa edelleen Ukrainaan, ja asejärjestelmiä ja ammuksia toimitetaan hitaasti mutta vakaasti itään, useimmat Euroopan maat ovat edelleen jäljessä energiaomavaraisuudessaan, itsenäisessä sotilaallisessa pelotteessaan ja sosiaalisen resilienssin tavoitteissaan. [12] Vaikuttaa siltä, että vallalla on eräänlainen taikausko. Nykyinen konflikti on ohi yhtenä päivänä, jota seuraa paluu uuteen normaaliin, keskinäiseen luottamukseen, kansainvälisen oikeuden tunnustamiseen ja hyvään järjestykseen.

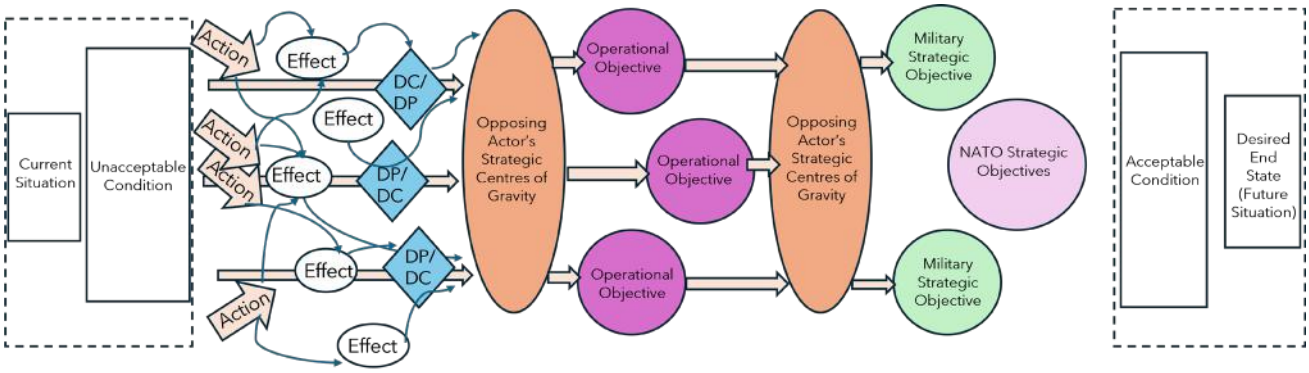
Venäjän avoimen sotaisa diplomaattinen, taloudellinen ja jopa sotilaallinen uhka ei ole vielä ylittänyt kynnystä tulla tunnustetuksi eksistentiaalisena uhkana, jollainen se on. [13] Poliittisissa lausunnoissa hahmotellaan itsestäänselvyyksiä. Sota ei ala joukkojen liikkeistä, taloudellisesta kiristyksestä, ydinaseilla lietsomisesta, kyberhyökkäyksistä, kohdennetuista murhista, vakoilusta ja ilmeisistä ihmisoikeusloukkauksista. Se ei ala strategisista pommikoneista ja tankeista, jotka ylittävät kansainvälisesti tunnustetut rajat. [14] [15] Sekä Kiinan kansantasavallan "rajoittamaton sodankäynti" että Venäjän "aktiiviset toimenpiteet" osoittavat tämän selvästi. [16] Vaikka länsimaiset johtajat haluaisivat soveltaa institutionalisoitua sodan määritelmää, nämä pyrkimykset ovat turhia niin kauan kuin toinen osapuoli päättää olla tunnustamatta niitä. Clausewitz vertasi sotaa kuuluisasti painiotteluun, jossa toinen osapuoli yritti pakottaa toisen alistumaan. [17] Kognitiivinen sodankäynti tekee juuri niin. Rauha edellyttää kahden osapuolen sitoutumista; sota vain yhden. Sodat alkavat, kun poliittiset johtajat tunnustavat ja julistavat (päättävät), että sota on alkanut. Jopa ilmeisen pahantahtoiset teot, jotka ovat tavanomaisen sodankäynnin kynnyksen alapuolella, on vaikea tunnistaa sotatoimiksi. Filosofia on kuitenkin todellisuuden edeltäjä ja historiallinen esimerkki: lukuisten saapuvien nuolien huomiotta jättämisellä voi välttää taistelun, mutta ei niiden tappavaa vaikutusta. Nuolet ovat todellisia, ja ne on suunnattu länteen.

Antagonististen voimien hyökkäykset tapahtuvat kognitiivisessa ulottuvuudessa. Kognitiivinen sodankäynti sisältää muiden vaikuttamiskeinojen kanssa synkronoituja toimintoja, joilla vaikutetaan asenteisiin ja käyttäytymiseen, suojelemalla tai häiritsemällä yksilön, ryhmän tai väestötason kognitiota edun saamiseksi vastustajaan nähden. Koko yhteiskunnan manipuloinnista on tullut uusi normi, joka on suunniteltu muokkaamaan todellisuuskäsityksiä. Ihmisen kognition muokkaaminen on kriittinen sodankäynnin alue. [18] Kun otetaan huomioon tämä määritelmä, miten sotilaskeinoilla voidaan torjua tai mielekkäästi tukea pyrkimyksiä torjua tällaista sodankäyntiä? Tulisiko olla uhmakkaan kärsivällinen vai suosia luovuutta sekavassa tilanteessa? Entä odottaako sotilaallista eskalaatiota vai ryhtyä kattaviin vastatoimiin?

KUN KÄYTÖSSÄ ON VAIN VASARA, ALKAA KAIKKI NÄYTTÄÄ NAULOILTA

Termi kognitiivinen sodankäynti soveltuu myös sotilasmaailmaan. Ihannetapauksessa valtiot johtavat armeijaa käydäkseen sotaa tai vastatakseen eksistentiaalisiin uhkiin. Näin ollen, jos kognitiivinen sodankäynti uhkaa eksistentiaalisesti valtiota hyökkäämällä sen sosiaalista yhteenkuuluvuutta vastaan, delegitimoimalla sen poliittisen johdon ja jopa puuttumalla jokaisen demokratian korkeimpaan hyvään – vaaleihin – sotilaallisia keinoja voidaan käyttää uhan torjumiseksi. Kognitiivinen sodankäynti yhdistää kyber-, informaatio-, psykologiset ja sosiaalisen manipuloinnin keinot,[19] jotka kaikki ovat saatavilla armeijoilla.

Ongelman ratkaisemiseksi useimmat länsimaiset armeijat noudattavat erillisiä suunnitteluvaiheita. Poliittiset tavoitteet muunnetaan sotilaallisiksi tavoitteiksi. Nämä tavoitteet edistävät määritellyn halutun lopputilan saavuttamista. Sotilaallisten ja täydentävien ei-sotilaallisten toimien luomat ratkaisevat ehdot ja vaikutukset määrittelevät etenemissuunnitelman sietämättömästä tilasta hyväksyttävään tilaan. [20]



Lähde: COPD [21]

Vaikka yhteistyöhön perustuvaan suunnitteluprosessiin kuuluu useita komentotasoja, mukaan lukien institutionaalinen luovuus ja asiantuntemus sekä todelliset teot paikan päällä, toimia määrittelevät (pääasiassa) sota-alueella taistelevat komennot. [22] Vaikka tälle sotatoimialueelle ei ole yhteisesti sovittua määritelmää, se voidaan määritellä organisaatiorakenteiksi, jotka käsittävät vastuualueen, jolla on ainutlaatuinen toimintaympäristö, joka vaatii erilaisia taktiikoita, varusteita ja rakennetta. [23] Samoin Nato määrittelee operatiivisen alueen "määritellyksi voimavarojen ja toimintojen alaksi, jota voidaan soveltaa sitoutumistilassa". [24]

Kognitiivista sodankäyntiä käydään epäilemättä (toiminnallisella eikä maantieteellisellä) vastuualueella ainutlaatuisessa toimintaympäristössä, nimittäin ihmismielessä. Laitteet ja rakenteet johdetaan tehtävistä ja taktiikoista. Kuitenkin nämä välttämättömät taktiikat ylittävät länsimaisten armeijoiden opilliset ja jopa lailliset rajoitukset. Länsimaiset sotilasdoktriinit sulkevat nimenomaisesti väestönsä vaikutusoperaatioiden ulkopuolelle. [25] Lisäksi sotilaalliset pyrkimykset muokata kansakuntien väestön ajattelua ovat selvästi länsimaisten yhteiskuntien oikeudellisten kehysten ulkopuolella. Ilmeisesti ei ole olemassa kognitiivista sodankäynnin aluetta; [26] Ja vaikka olisikin, länsimaisia armeijoita kiellettäisiin toimimasta siinä omaa väestöään vastaan.

Lisäksi tällaisessa toimintaympäristössä sotilaallinen terminologia vaikuttaa liian ehdottomalta ja liian monimutkaiselta. Termit kuten ylivalta ja paremmuus merkitsevät eräänlaista kiistatonta määräävää asemaa vastaavissa ulottuvuuksissa. Digitalisaation aikakaudella tieto liikkuu vapaasti verkossa eurooppalaisten arvojen mukaisesti. Tässä yhteydessä kyberavaruus on sekä disinformaation että informaation ja kognitiivisen sodankäynnin alusta ja väline. Kyberulottuvuus on olennaisesti helpottanut läpinäkyvän ihmisen ja läpinäkyvän yhteiskunnan luomista. Digitalisaatio ja kyberavaruuden jokapäiväinen käyttö ovat muuttaneet tämän keinotekoisen alueen todellisten seurausten paikaksi, diplomaattiseksi välineeksi, taloudelliseksi tekijäksi, sotilaalliseksi vaikuttajaksi ja sosiaaliseksi tilaksi, joka tyydyttää esimerkiksi ihmisten sosiaalisia tarpeita. Kyberavaruus on edistänyt tiedon demokritisoitumista ja antanut pahantahtoisille toimijoille mahdollisuuden vaikuttaa kohdeyleisöihin, asettaa ja hallita narratiiveja sekä hyödyntää tietoa. [27] Mikään absoluuttinen ylivalta kognitiivisessa ulottuvuudessa ei käytä pääasiassa demokratisoitua kyberavaruutta.

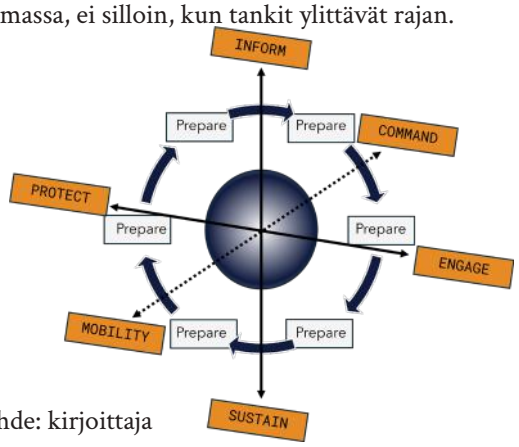
Ukrainassa käynnissä oleva sota on korostanut korbettilaisemman lähestymistavan hallitsevaa asemaa, mikä tarkoittaa tarvetta saavuttaa riittävän hyvät olosuhteet, jotta tiettyä (toiminnallista) aluetta voidaan hyödyntää parhaalla mahdollisella tavalla tietyn ajanjakson ajan. [28] Tämä puolestaan näyttää olevan saavutettavissa sekä käytännössä että oikeudellisesti, koska tavoitteena ei ole sosiaalinen indoktrinaatio eikä pysyvä kognitiivinen yhdenmukaistaminen. On kuitenkin kyseenalaista, onko armeija väline tähän.

Sotilaskeinot ovat kansakunnan toimeenpaneva lähestymistapa ulkoisiin uhkiin. Tämä seikka erottaa sen selvästi sisäisesti suuntautuneista poliisivoimista. [29] Armeijan tehtävä joko käydä tai torjua kognitiivista sodankäyntiä näyttää ilmeiseltä, mutta turhalta valinnalta. Vaikka asianmukaiset suunnittelumekanismit ovat käytössä, armeijan ominaisuudet tai demokraattisesti legitiimi kehys ja organisaatiokulttuuri kansakunnan eksistentiaalisena vartijana eivät tee siitä oikeaa työkalua tehtävään. Kognitiiviset sotaprikaatit eivät ratkaise ongelmaa. He taistelisivat pimeässä uhmakkaasti ja kärsivällisesti, rajoittuneina, huonosti varustettuina, epäasianmukaisesti koulutettuina ja lopulta saavuttamatta toivottua vaikutusta.

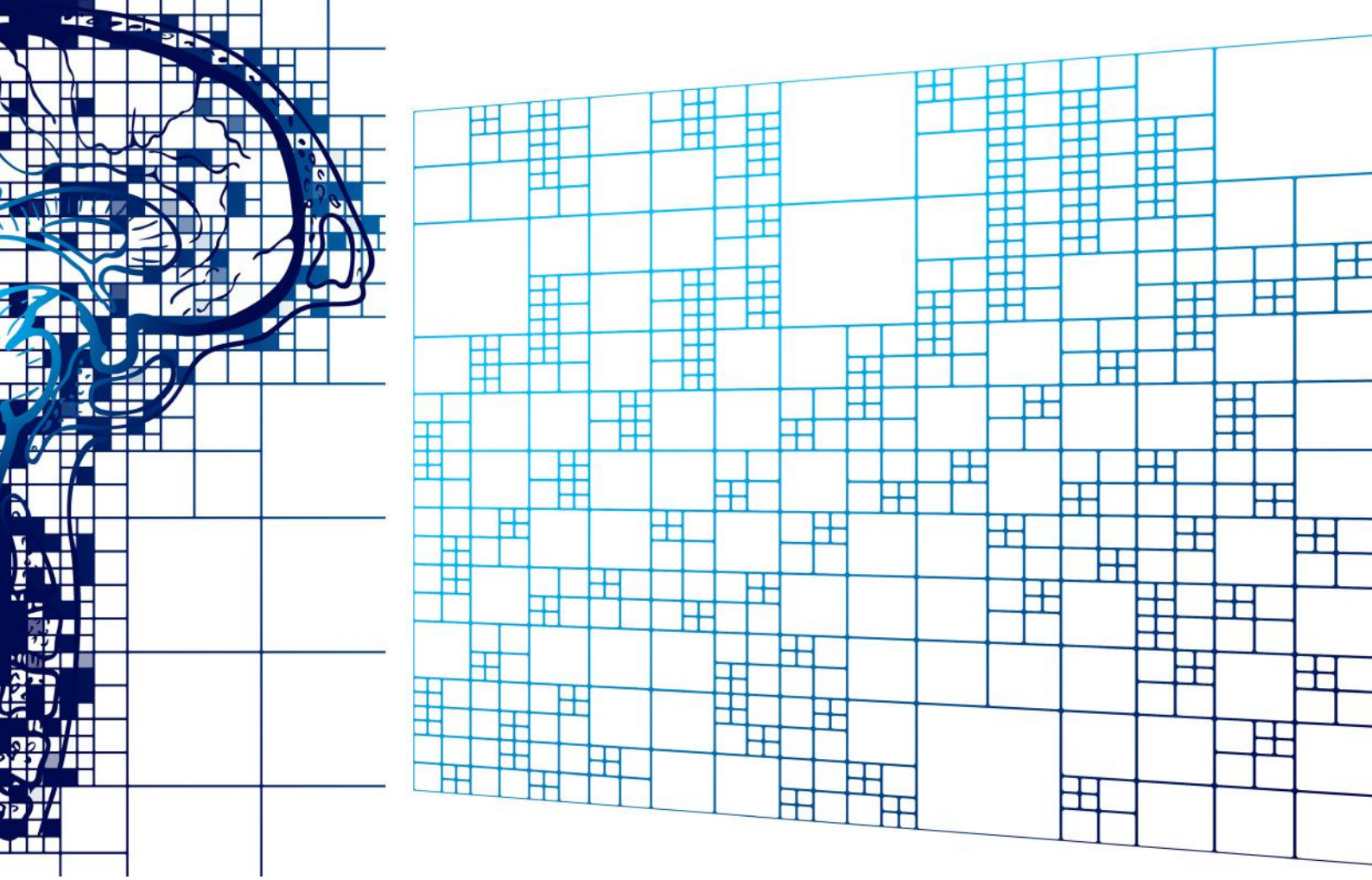
ETUA EPÄSELVYYDESSÄ

Kognitiivista sodankäyntiä on käytävä synkronisesti muiden keinojen kanssa asenteisiin ja käyttäytymiseen vaikuttamiseksi. Sotilaallinen sodankäyntialue ja sen ulottuvuudet, kuten kyberavaruus, sähkömagneettinen spektri ja informaatiotila, ovat vain käsitteen pintapuoli. Uhka on kokonaisvaltaisempaa kuin pelkkää teknistä hakkerointia, ja se vahingoittaa yhteiskuntiamme kokonaisvaltaisesti. Demokratioita heikennetään heikentämällä sekä ihmisten luottamusta politiikkaan että heidän halukkuuttaan puolustaa elämäntapaamme. Samalla haastetaan oikeudellinen ja eettinen kehys hyödyntämällä länsimaiden sitoutumista oikeusvaltioperiaatteeseen ja liberalismiin. Lisäksi enemmän tai vähemmän järkevien epäilysten herättäminen, vaihtoehtoiset totuudet ja uskottava kiistäminen kohdistuvat ihmisen psykologiaan ja kognitioon informaation aikakaudella. Kaikki nämä pyrkimykset johtavat geopoliittisiin muutoksiin, jotka syrjäyttävät Euroopan aseman maailmannäyttämöllä. [30] Kokonaisvaltaiset haasteet vaativat kattavia vastauksia! Ongelmaan ei siis löydy ratkaisua yhdestä kovan voiman välineestä.

Kognitiivisen sodankäynnin torjuminen ja tehokas reagointi siihen tarvittaessa (ja sen merkityksen ymmärtäminen sotilaallisen suunnittelun ja operaatioiden toteuttamisessa) on pääasiassa varautumista. Kaikki sotilaallisen voimavaran aspektit – johtaminen, toiminta, ylläpito, liikkuvuus, suojelu ja tiedottaminen – perustuvat asianmukaiseen valmisteluun. Kognitiivisen sodankäynnin vastustaminen johtaa väistämättä taisteluun narratiivisesta valta-asemasta, "absoluuttisesta totuudesta" ja paremmasta tulkinnasta. [31] Valitettavasti länsimaisten yhteiskuntien on täytynyt oppia, että "tosiasiallisella totuudella" sinänsä ei ole merkitystä. Kun narratiivi hallitsee informaatiomaailmaa, ihmisten ajattelutapa on jo muotoutunut. Esimerkit tästä ilmiöstä vaihtelevat tunnetusta (mutta olemattomasta) lupauksesta Gorbatšoville entisten Varsovan liiton valtioiden asemasta suhteessa Natoon, Vladimir Putinin historiallisiin (mutta merkityksettömiin ja joskus jopa absurdeihin) väitteisiin Ukrainasta. [32] [33] [34] Subjektiivinen totuus, jolla ainoastaan on merkitystä yksilöille, on ihmisten uskomuksissa. "Totuus" piilee ihmisen käsityksessä, ja sota tapahtuu, kun poliitikot sanovat, että sota on olemassa, ei silloin, kun tankit ylittävät rajan.



Lähde: kirjoittaja



Venäjä on ollut sodassa lännen kanssa siitä lähtien, kun Vladimir Putin totesi tämän julkisesti useaan otteeseen, muun muassa Münchenin turvallisuuskonferenssissa vuonna 2008. [35] Se on sota, jota ei vieläkään käydä aktiivisesti sotilaallisin keinoin Ukrainan ulkopuolella. Tämän pitäisi puolestaan tarkoittaa, että myös länsi on sodassa. Poliittisten johtajien on kohdattava tämä epämukavuus ja hyväksyttävä se tosiasiana. Se ei ole sota, jonka länsi päätti käydä. Se on sota, joka pakotettiin lännelle, riippumatta siitä, kuinka räikeästi Vladimir Putin pyörittelee tosiasioita. Länsimaisten yhteiskuntien tulisi siksi varmistaa sekä sotilaallinen pelote että sosiaalinen sietokyky kaikilla aloilla ja ulottuvuuksissa sekä hyödyntää strategista epäselvyyttä. Yhteiskunta, joka on hyvin perillä sotatilasta (erityisesti sellaisesta, jota ei käydä sotilaallisin keinoin), on halukkaampi kehittämään, tukemaan ja edistämään pelotetta ja selviytymiskykyä. [36]

Valtavasti työtä on vielä tehtävä sellaisilla aloilla kuin koulutus (esim. henkinen maanpuolustus, kansallinen turvallisuus- ja puolustuspolitiikka, eurooppalaiset arvot), valtiollinen, puolivaltiollinen talous ja siviilitalous (strateginen autonomia, kansallinen varastointi), yhteiskunta (sosiaalinen yhteenkuuluvuus, moniarvoisuus, osallisuus ja monimuotoisuuden hallinta) ja tietotekniikka (sosiaalisen median arvo ja kirous, digitaalinen lukutaito). Sotilaallista osallistumista tarvitaan kuitenkin myös. Armeijat ovat kehittäneet historian aikana prosesseja ja menettelyjä, jotka toimivat pahimmissa kuviteltavissa olevissa olosuhteissa ja tarjoavat silti toteuttamiskelpoisia ratkaisuja.

Demokratioilla on puutteita strategisten tavoitteiden määrittelyssä. [37] Armeija pystyy tarjoamaan menettelytapoja saavutettavissa olevien tavoitteiden kehittämiseksi ja laatimiseksi. [38] Kansakunnan antureita on paljon ja viestintälinjat niin laajoja ja monimutkaisia, että tilannetietoisuuden saavuttaminen on vaativaa. Armeijat ovat kuitenkin kehittäneet konsepteja monimutkaisuuden ja komplikaatioiden käsittelemiseksi. [39] Yhteiskuntien väliset ja sisäiset suhteet ja yhteydet ovat monikerroksisia ja niitä muokkaavat muun muassa historia, kulttuuri ja uskonto, joten on haastavaa saada ja ylläpitää kattavaa ymmärrystä sosiaalisesta vuorovaikutuksesta.

Asevoimat ovat kuitenkin kehittäneet tekniikoita, joilla luodaan keinojen ja voimavarojen puitteissa kattava käsitys asiaankuuluvista toimijoista, niiden eduista, vahvuuksista, heikkouksista ja keskinäisistä yhteyksistä myös alueen ulkopuolisissa operaatioissa. [40] Luontaisen tarpeen kautta armeijat pystyvät muotoilemaan ongelmia ja määrittelemään tehokkaita lähestymistapoja, rakenteita, organisaatioita ja viime kädessä toteuttamiskelpoisia toimintatapoja. Asevoimilla on tarvittavat välineet vaikutusten ja kohdeyleisöjen määrittelemiseksi, riskien

ja asianmukaisten lieventävien toimenpiteiden arvioimiseksi sekä edistymisen mittaamiseksi edetessään hyväksymättömästä tilasta hyväksyttävään tilaan. Heillä on kaikki nämä työkalut ja he voivat tarjota niitä päätöksentekijöille, vaikka he eivät olisikaan johtava vallan väline.

Tämä ei tietenkään ole kehotus elvyttää militarismia. Lisäksi korostaessaan poliittisen valvonnan tarvetta sotilaalliseen vallan välineeseen nähden, Carl von Clausewitz mainitsi nimenomaisesti suvereenin tarpeen arvostaa sotilasasiantuntijoiden parhaita neuvoja. [41] Kun Clausewitz kirjoitti Sodasta, hän teki sen suvereniteetin näkökulmasta, joka hallitsi vain yhtä vallan välinettä, armeijaa. Voimme olettaa, että jos olisi ollut olemassa muitakin voimia, hän olisi laajentanut teoriansa armeijan lisäksi muihin vallan välineisiin.

Vaikka sotaa voidaan käydä muilla välineillä kuin armeijalla, armeija voi tarjota tukea vastauksena ei-kineettisiin / kynnyksen alittaviin uhkiin, kuten kognitiivisiin uhkiin. Tällöin on todellakin elintärkeää, ettei yhteiskunnasta tule militaristista. Sotilaallisen kovan voiman lisäksi keskeinen pelotetekijä on pehmeän vallan ylläpitäminen ja jopa laajentaminen – nimittäin eurooppalaiset arvot, vapaus ja monimuotoisuus. [42] Antagonistinen valta ei pelkää mitään enemmän kuin avointa liberaalidemokraattista järjestelmäämme. [43] Liberaali demokratia hylkää heidän valtakoneistonsa perustan ja lopulta delegitimoi heidän hallintonsa. Varjossa taisteleminen mahdollistaa strategisen epäselvyyden hyödyntämisen. Tarvittavat varautumistoimenpiteet voidaan toteuttaa varjossa paahtavan auringon sijaan.

TAISTELUA VARJOISSA

Ongelman ratkaisemiseksi on tunnustettava, että sellainen on ylipäätään olemassa. Sen huomiotta jättäminen johtaa väistämättä tappioon. Kun länsimaiset yhteiskunnat ottavat ratkaisevan askeleen, poliittisten johtajien on päätettävä, miten käsitellä näitä moniulotteisia eksistentiaalisia uhkia: löytämällä etu myllerryksestä tai olemalla uhmakkaan kärsivällinen. Kaikenlaisen sodankäynnin valmistelun liittäminen kansakunnan sotataisteluvälineeseen näyttää ilmeiseltä ratkaisulta. Johtajien tulisi olla tietoisia sotilaallisesta sopeutumiskyvystä ja luontaisesta kuuliaisuudesta. Tämä vallan väline ottaa varmasti tehtävän vastaan ja täyttää sen keinojensa ja kykyjensä puitteissa. Vaikka olemmekin kuinka mukautumiskykyisiä, on olemassa vaara, että vasara kohtelee ongelmaa kuin naulaa, varsinkin kun otetaan huomioon oikeudelliset rajoitukset. Kärsivällisyydessä armeija taistelisi reaktiivisesti molemmat kädet sidottuina selän taakse ulottuvuudessa, joka vaati kattavampaa lähestymistapaa.

Onneksi nykyaikaisella valtiolla on enemmän kuin vain yksi vallan väline. Koordinoituina ja synkronoituina, laillistettujen demokraattisten johtajien valvonnassa he voivat saavuttaa tehokkaimmat tulokset neuvotteluissa. Armeijan roolin tässä orkesterissa pitäisi olla kaksijakoinen. Toisaalta sen on täytettävä olemassaolonsa tarkoitus – nimittäin pelotevaikutus. Toisaalta se voi tarjota arvokkaita prosesseja, menettelyjä ja tekniikoita sekä poliittiselle johdolle että muille vallan välineille.

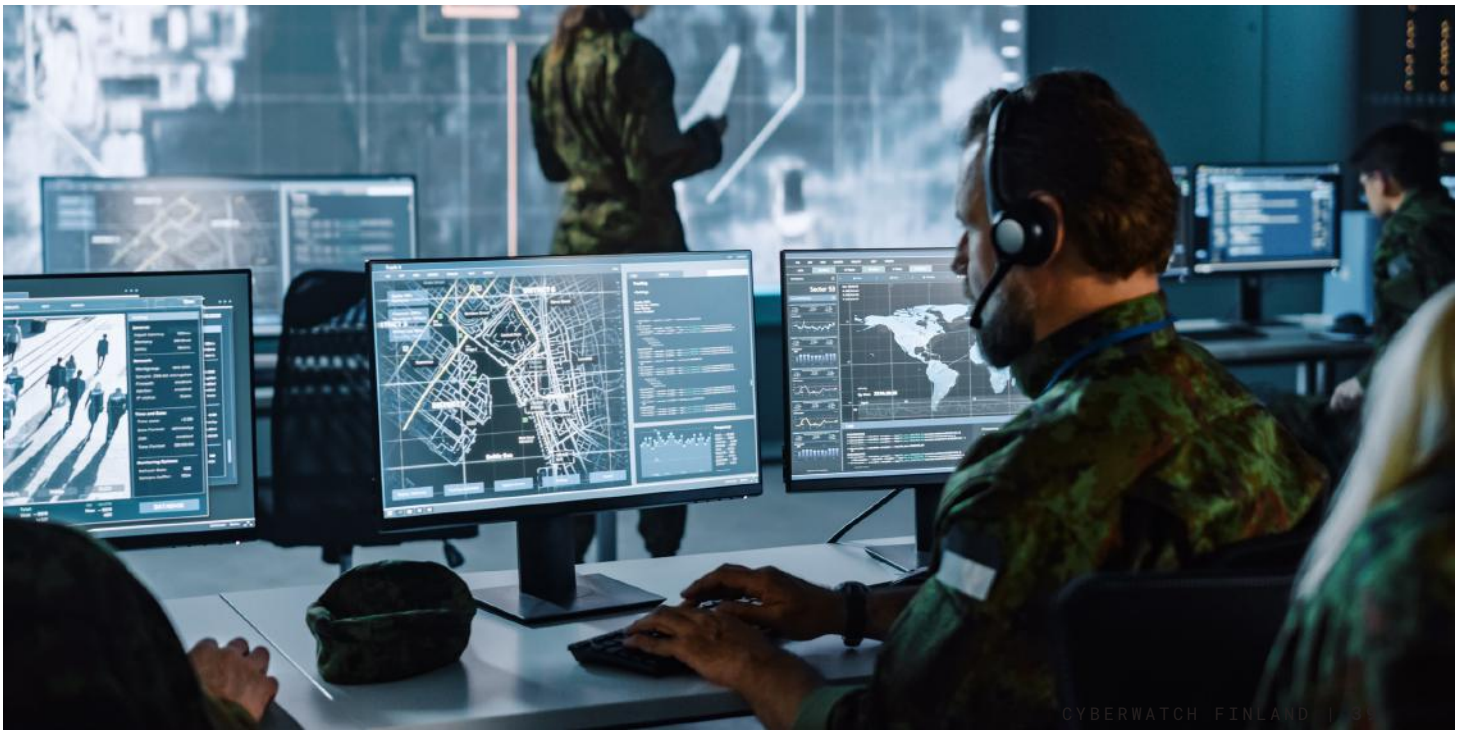
Viime kädessä on pidettävä mielessä, että kognitiivinen sodankäynti kohdistuu pääasiassa siviileihin, demokraattiseen suvereniteettiin. Tämä ei ole uusi ilmiö. Noin sata vuotta sitten, kun Giulio Douhet käsitteli ilmavoimia ja sotilaallisia syviä operaatioita, hän kirjoitti: "Sotilaiden ja siviilien välillä ei enää ole eroa. Maa- ja meripuolustuksella ei enää suojella niiden takana olevaa maata; eikä voitto maalla tai merellä voi suojella ihmisiä..."[44] Ihmiskunta on löytänyt ratkaisun ongelmaan kansainvälisestä oikeudesta. Tämä ei tarkoita, että kognitiivisen sodankäynnin lännelle asettamiin haasteisiin olisi olemassa oikeudellinen ratkaisu. On todennäköisempää, että se on sysäys yhteiskuntien jatkokoulutukselle tai hallitusten tietotaitojen kehittämiselle. Tavalla tai toisella näyttää väistämättömältä, että Euroopan on jälleen puolustettava olemassaoloaan ja arvojaan taistelemalla varjossa. ■

MATTHIAS WASINGER

Matthias Wasinger on yleisesikunta eversti Itävallan asevoimissa. Hänellä on maisterintutkinto sotilasjohtamisesta (Theresan Military Academy), maisterin tutkinto operatiivisista opinnoista (US Army Command and General Staff College) ja tohtorin tutkinto monitieteisistä opinnoista (Interdisciplinary Studies, Wienin yliopisto). Hän on palvellut sekä kansainvälisesti että kansallisesti kaikilla komentotasoilla. Hän on myös The Defence Horizon Journal -aikakausilehden perustaja ja päätoimittaja. Hän on palvellut Naton kansainvälisen esikunnan päämajassa Brysselissä vuodesta 2020. Tässä artikkelissa esitetyt näkemykset ovat yksin kirjoittajan omia näkemyksiä.

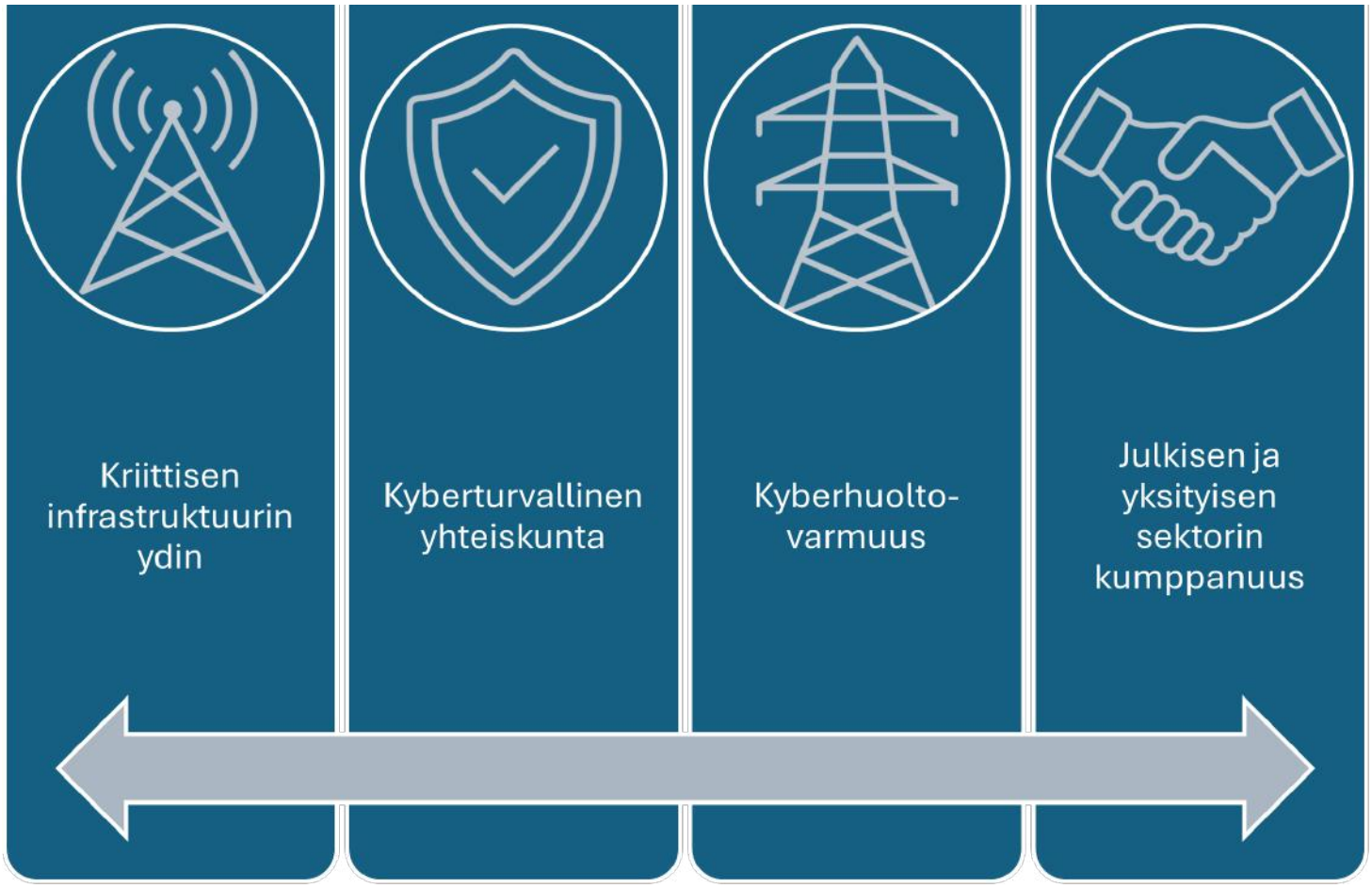
LÄHTEET:

[1] Herodotus, The Histories Book 7: Polymnia (Start Publishing LLC, 2015).
[2] Plutarch, Apophthegmata Laconica (Loeb Classical Library edition, Vol III, 1931).
[3] Valerius Maximus, Factorum et dictorum memorabilium, liber III.
[4] Peter Dickinson, 'Putin's Poisonous Anti-Western Ideology Relies Heavily on Projection', Atlantic Council, 3 July, 2022, accessed 7 March, 2024, https://www.atlanticcouncil.org/blogs/ukrainealert/putins-poisonous-anti-western-ideology-relies-heavily-on-projection/.
[5] Matthias Wasinger, 'The Highest Form of Freedom and the West's Best Weapons to Counter Cognitive Warfare', TDHJ.org, accessed 21 May, 2024, https://tdhj.org/blog/post/freedom-counter-cognitive-warfare/.
[6] Robert Seely, 'Defining Contemporary Russian Warfare', The RUSI Journal Volume 162, Issue 1 (2017): https://doi.org/10.1080/03071847.2017.1301634.
[7] Akaki Dvali, 'From Appeasement to Accountability – The West's New Approach Can Save Georgia from Putin', Newsweek, 19 March, 2024, accessed 11 May, 2024, https://www.newsweek.com/appeasement-accountability-wests-new-approach-can-save-georgia-putin-opinion-1880600.
[8] Hodun, Milosz and Cappelletti, Francesco, eds, Putin's Europe: Russia's Influence in European Democracy (ELF, 2023), 176–177.
[9] Geoffrey Roberts, '"Now or Never": The Immediate Origins of Putin's Preventative War on Ukraine', Journal of Military and Strategic Studies Volume 22, Issue 2 (2022).
[10] Ian Garner, 'The West Is Still Oblivious to Russia's Information War', Foreign Policy, 2024, accessed 11 May, 2024, https://foreignpolicy.com/2024/03/09/russia-putin-disinformation-propaganda-hybrid-war/.
[11] Congressional Research Service, Russia's War Against Ukraine: European Union Responses and U.S.-EU Relations (2024), https://crsreports.congress.gov/product/pdf/IN/IN11897.
[12] Council of the European Union, '"If We Want Peace, We Must Prepare for War"', news release, 19 March, 2024, accessed 11 May, 2024, https://www.consilium.europa.eu/en/press/press-releases/2024/03/19/if-we-want-peace-we-must-prepare-for-war/.
[13] Michael P. o. Liechtenstein, 'Is a Broader European War Imminent?', GIS, 2024, accessed 11 May, 2024, https://www.gisreportsonline.com/r/is-european-war-imminent/.
[14] Rosa Brooks, 'Can There Be War Without Soldiers?', Foreign Policy, 2016, accessed 11 May, 2024, https://foreignpolicy.com/2016/03/15/can-there-be-war-without-soldiers-weapons-cyberwarfare/.
[15] Seth G. Jones, Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare (New York, NY: W. W. Norton & Company, 2021), 73–76.
[16] Seth G. Jones, Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare (New York, NY: W. W. Norton & Company, 2021).
[17] Carl von Clausewitz, On War, ed. Michael Howard Princeton, NJ [u.a.]: Princeton Univ. Press, 1989, 75.
[18] Allied Command Transformation, Cognitive Warfare (2024), accessed 10 February, 2024, https://www.act.nato.int/activities/cognitive-warfare/.
[19] Idem.
[20] Allied Command Transformation, Comprehensive Operations Planning Directive: COPD INTERIM V2.0, 4–32 – 4–110.
[21] Ibid., 4–53.
[22] Ibid., 4–32 – 4–110.
[23] Everett C. Dolman, 'Space Is a Warfighting Domain', ÆTHER: A JOURNAL OF STRATEGY & AIRPOWER 1, Volume 1 (2022): 84, accessed 10 March, 2024, https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-1_Issue-1/11-Dolman.pdf.
[24] Allied Joint Publication-01, AJP-01 (NATO), no. 01, LEX-06.
[25] AJP-3.10, Allied Joint Doctrine for Information Operations (NATO), no. 3.10, 1–2 – 1–10.
[26] Patrick Hofstetter and Flurin Jossen, 'There Is No Need for a Cognitive Domain', TDHJ.org, 2 November, 2023, accessed 13 May 2024, https://tdhj.org/blog/post/no-need-cognitive-domain/.
[27] Matthias Wasinger, 'The Highest Form of Freedom and the West's Best Weapons to Counter Cognitive Warfare', TDHJ.org, accessed 21 May, 2024, https://tdhj.org/blog/post/freedom-counter-cognitive-warfare/.
[28] Julian S. Corbett, Some Principles of Maritime Strategy: A Theory of War on the High Seas; Naval Warfare and the Command of Fleets (Adansonia Press, 2018), 71–141.
[29] Matthias Wasinger, 'Vom Wesen und Wert des Militärischen: Interdisziplinäre Reflexion zum Alleinstellungsmerkmal des Militärischen zwischen Anspruch und Wirklichkeit' (Dissertation, Faculty of Law, 2017), 54–55.
[30] Matthias Wasinger, 'The Highest Form of Freedom and the West's Best Weapons to Counter Cognitive Warfare', TDHJ.org, accessed 21 May, 2024, https://tdhj.org/blog/post/freedom-counter-cognitive-warfare/.
[31] See for example: Government of Canada, 'Countering Disinformation with Facts – Russian Invasion of Ukraine', Government of Canada, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng.
[32] Jeff Neal, '"There Was No Promise Not to Enlarge NATO" – Harvard Law School', Harvard Law School, accessed 14 May, 2024, https://hls.harvard.edu/today/there-was-no-promise-not-to-enlarge-nato/.
[33] NATO, 'NATO – Official Text: Founding Act on Mutual Relations, Cooperation and Security Between NATO and the Russian Federation Signed in Paris, France, 27 May 1997', accessed 13 May 2024, https://www.nato.int/cps/su/natohq/official_texts_25468.htm.
[34] Government of Canada, 'Countering Disinformation with Facts – Russian Invasion of Ukraine', Government of Canada, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng.
[35] Nick Fishwick, 'Putin Has Declared War on the West. It's Time to Take the Fight to Russia', The Cipher Brief, 19 February, 2024, accessed 9 May, 2024, https://www.thecipherbrief.com/column_article/putin-has-declared-war-on-the-west-its-time-to-take-the-fight-to-russia.
[36] Michal Onderco, Wolfgang Wagner, and Alexander Sorg, WHO ARE WILLING to FIGHT for THEIR COUNTRY, and WHY? (2024), accessed 7 May, 2024, https://spectator.clingendael.org/en/publication/who-are-willing-fight-their-country-and-why.
[37] Donald J. Stoker, Why America Loses Wars: Limited War and US Strategy from the Korean War to the Present, Revised and updated [edition] (Cambridge: Cambridge University Press, 2022), 53–60.
[38] Allied Command Transformation, Comprehensive Operations Planning Directive: COPD INTERIM V2.0, 3–19 – 3–36.
[39] NATO Science and Technology Organization, 'Visualisation and the Common Operational Picture', accessed 13 May, 2024.
[40] Allied Command Transformation, Comprehensive Operations Planning Directive: COPD INTERIM V2.0, 4–13 – 4–48.
[41] Carl von Clausewitz, On War, ed. Michael Howard, (Princeton, NJ [u.a.]: Princeton Univ. Press, 1989), 608–609.
[42] Robert Service, The Penguin History of Modern Russia: From Tsarism to the Twenty-First Century, 4th ed. (London, UK: Penguin, 2021), 571–591.
[43] Timothy Frye, Weak Strongman: The Limits of Power in Putin's Russia (Princeton and Oxford: Princeton University Press, 2021), 12–14.
[44] Giulio Douhet, The Command of the Air, USAF warrior studies Washington, D.C.: Air Force History and Museums Program, 1942, 10.



CYBERWATCH FINLAND – MODERNIN DIGITAALISEN YHTEISKUNNAN HAASTEET JA RESILIENSSI

TIIVISTELMÄ WHITE PAPERISTA



Kuva 1. Kriisinkestävän yhteiskunnan neljä peruspilaria.

Kansainvälisen toimintaympäristön muutos ja digitalisoituminen haastavat länsimaisia yhteiskuntia nostaen esiin uusia haasteita ja kehittämistarpeita. Venäjän Ukrainaan kohdistama hyökkäyssota ja muu kyberaktiivisuus ovat avanneet silmiä laajalti. Lisäksi kasvava kyberturvallisuussääntely tulee lisäämään organisaatioiden turvallisuusvastuita myös tällä osa-alueella. Syksyn merkittävin uutinen on NIS2-direktiivin voimaan tulo Euroopassa. Vuoden 2024 aikana valmistelussa on myös useita merkittäviä kyberselontekoja ja strategioita.

Kybertoimintaympäristö onkin jatkuvan muutoksen keskellä. Strategisen kyberturvallisuuden asiantuntijatalo Cyberwatch Finland, seuraa ja tuottaa aktiivisesti kybertilannekuvaa. Tätä tietoa haluamme jakaa myös laajemmin. Yhteiskunnan kokonaisvaltaisen turvallisuuden kehittämiseksi tiedon siiloutumista tulisi välttää ja hyviä käytäntöjä levittää laajalle. Kyberala kaipaa myös uusia ideoita ja oppia vanhasta, sekä rakentavaa keskustelua kyberturvallisuuden kehittämisestä.

Tätä taustaa vasten Cyberwatch Finland julkaisi elokuussa 2024 white paperin modernin digitaalisen yhteiskunnan haasteista ja resilienssistä. Tavoitteenamme on herättää keskustelua kyberturvallisuuden tilasta sekä jakaa keräämiämme oppeja viime vuosien ajalta. Suomessa, valitettavasti, yksityisen sektorin rooli aloitteiden tekijänä on jäänyt marginaaliin. Varsinainen ajatuspajatoiminta on maassamme vähäistä ja sille voisi olla laajempaakin tilausta. Näin ollen white paper itsessään on oiva formaatti uusille ajatuksille ja aloitteille. Tarkoituksenamme ei ole arvostella ketään vaan ajatella ääneen.

White paperin avulla haluaisimme ensinnäkin kiinnittää huomiota Ukrainan sodan aiheuttamaan muutokseen paitsi kybertoimintaympäristössä, myös turvallisuusympäristössämme laajemminkin. Sodankäynnin paradigma on merkittävästi muuttunut. Erilaista hybridivaikuttamista ja häirintää tapahtuu kasvavissa määrin varsinaisen sodan kynnyksen alapuolella, mikä muodostaa moninaisia haasteita, joihon on vaikea vastata. Sodankuva on myös muuttunut. Fyysisen, niin kutsutun kineettisen vaikuttamisen rinnalle ovat nousseet ei-kineettiset operaatiot, kuten kyberoperaatiot ja psykologinen vaikuttaminen eri muodoissaan, esimerkiksi valeuutisina ja muina ihmisten kognitiiviseen toimintakykyyn vaikuttavina keinoina. Ukrainan sota on ensimmäinen digi- ja someaikakauden sota Euroopassa. Sen oppeja, tullaan varmasti käymään läpi tulevina vuosina ja jälkijättöisesti sodan loputtua. Tärkeä on myös oppia lennosta ja jo kriisin ollessa käynnissä.

Toisena avainviestinä yhä tärkeämmäksi on nousemassa yhteiskunnan kriittisten rakenteiden, niin kutsutun kriittisen infrastruktuurin suojaaminen uhkilta, mukaan lukien kyberuhkilta. Digitalisoituminen ja esineiden internet johtavat kriittisten järjestelmien kasvavaan liittämiseen verkkoon. Tähän infrastruktuuriin Venäjä on kohdistanut kineettistä sekä ei-kineettistä vaikuttamistaan Ukrainassa. Kyberhyökkäysten kohteina ovat olleet muun muassa maan energiasektori, tietoliikennesektori, media sekä logistiikka-alan toimijat.

Digitalisaation myötä nouseviin ja kriittisen infrastruktuuriin kohdistuviin uhkiin varautuminen edellyttää että, kriittisen infrastruktuurin selkeää määrittelyä. Globaalisti tarkasteltuna määritelmiä on monia, jopa satoja. EU:n mukaan kriittisiä infrastruktuureja ovat sähköverkko, liikenneverkko sekä tieto- ja viestintäjärjestelmät. Suomessa kriittistä infrastruktuuria ei ole määritelty, työ on vasta aloitettu. Kriittisestä infrastruktuurista keskusteltaessa, ja uhkiin varautuessa, tulisi korostaa erityisesti sen ydintä: sähköverkkoa, tietoliikenneyhteyksiä sekä paikkatiedon ja tarkan ajan tuottavia satelliittijärjestelmiä. Ilman näitä modernit yhteiskunnat eivät toimi ja lisäksi nämä kokonaisuudet ovat toisistaan keskinäisriippuvaisia.

Konkreettisina toimenpide-ehdotuksina esitämme. että Suomessa tulisi määritellä kansallisen kriittisen infrastruktuurin ydin osana kansallista kriittistä infrastruktuuria ja palveluja ja näin parantaa kokonaisuuden hallintaa kriittisen infrastruktuurin osalta. Edelleen tälle kriittiselle infrastruktuurille tulisi laatia oma erityinen kyberturvallisuusohjelma, jossa otetaan huomioon sekä ei-kineettinen ja kineettinen vaikuttaminen eri valmiustiloissa ja häiriötilanteissa. Kriittisen infrastruktuurin toimijoiden uhka- ja riskitietoisuutta tulisi parantaa sekä tehostaa toimenpiteitä EU-regulaation vaatimusten toimeenpanossa.

Kolmanneksi Ukrainan sodan oppien ja kriittisen infrastruktuurin huomioimisen lisäksi, huomiota tulisi kiinnittää Suomessa kyberalan johtamiseen ja kyberhuoltovarmuuteen. Tämä voisi tarkoittaa esimerkiksi kyberturvallisuuden johtamismallin ja johtovastuiden selkeyttämistä. Tällä hetkellä kyberosaaminen ja johtaminen on

hajautunut useiden eri hallinnon aloille. Samalla tämä voisi tarkoittaa kattavan ja pitkäaikaisen teknologia/huoltovarmuusohjelman perustamista ei-kineettiseen toimintaympäristöön sekä kansallisen kyberturvallisuuden huoltovarmuusekosysteemin ja kansainvälisen kumppanuusverkoston vahvistamista.

Neljänneksi kriittisen infrastruktuurin suojaaminen ja yhteiskunnallisen resilienssin parantaminen eivät voi olla pelkästään julkisen sektorin varassa. Toimenpiteistä tulisi keskustella monitahoisesti ja ratkaisukeskeisessä hengessä. Yhdistämällä Ukrainan sodan opit, tunnistamalla kriittisen infrastruktuurin merkityksen sekä parantamalla kyberturvallisuuden johtamismalleja ja kyberhuoltovarmuutta luomme kyberturvallisemman yhteiskunnan. Tässä julkisen ja yksityisen sektorin kumppanuuksilla on keskeinen rooli. Kansallinen kyberturvallisuus edellyttää laajaa ja tiivistä yhteistyötä viranomaisten, kolmannen sektorin, järjestöjen ja elinkeinoelämän kesken. Yhteistyö voi tarkoittaa hyvinkin erilaisia toimintatapoja ja muotoja, mutta selkeiden rakenteiden ja pitkäjänteisyyden tulisi olla siinä avainasemassa. Konkreettisesti yhteistyö voisi tarkoittaa esimerkiksi julkisen sektorin ja yksityisen sektorin keskitettyjä, toimintavarmoja ja kustannustehokkaita kyberturvallisuuspalveluja, riskianalyysien ja tilannekuvan vaihtoa sekä analysointimekanismeja tai yhteisiä varautumissuunnitelmia kyberhuoltovarmuuden ylläpitämiseksi.

Kyberturvallisuuden kehitys ja parannukset eivät tapahdu itsestään sormia napsauttamalla. Kyberriskianalyysin kehittäminen, johtovastuiden selkeyttäminen, Ukrainan sodan oppien jalostaminen, kyberjohtamisen ja huoltovarmuuden kehittäminen sekä yhteiskunnan eri sektorien välinen yhteistyö ovat tärkeitä rakennuspalikoita yhteiskunnan kokonaisvaltainen kyberturvallisuuden kehittämisessä. Suomalaisen yhteiskunnan pitkäaikainen valtti on ollut yhteiskunnallinen luottamus viranomaisten ja kansalaisten kesken. Ottamalla tästä mallia myös kyberalalla, voimme yhdessä rakentaa resilienttiä ja kriisinkestävää yhteiskuntaa. Konkreettisia askeleita tätä varten esitämme julkaisemassamme white paperissa: https://www.cyberwatchfinland.fi/post/white-paper-modernin-digitaalisen-yhteiskunnan-haasteet-ja-resilienssi. ■

KUUKAUSIKATSAUS LOKAKUU/2024

// Cyberwatchin analyysitiimi

SISÄLLYS:

1. TAPAHTUMIA KYBERMAISEMASSA

2. VALOKEILASSA
   2.1. Onnistuneet viranomaisoperaatiot alleviivaavat viestiliikenteen turvallisuuden tärkeyttä
   2.2. Teknologiayhtiöt ja sosiaalisen median jätit negatiivisesti esillä syyskuussa
   2.3. Salasanakäytännöt muuttuvat

3. NÄITÄ KANNATTAA SEURATA
   3.1. Yhdysvaltojen presidentinvaalien lähestyessä vaalivaikuttaminen kiihtyy
   3.2. Kvanttisuojatut standardit ovat valmiita ja implementointi voi alkaa

TÄSSÄ KATSAUKSESSA

Tässä kuukausikatsauksessa tarkastelemme edellisen kuukauden merkittävimpiä kybermaailman ilmiötä ja sidomme ne laajempiin kokonaisuuksiin. Katsaus jakautuu kolmeen tarkastelukulmaan: kuukauden merkittävämpiin kybermaailman tapahtumiin, ilmiöihin, joita haluamme erityisesti korostaa sekä kokonaisuuksiin, joiden kehitystä kannattaa seurata.

Syyskuussa kybermaailmassa huomio kiinnittyi erityisesti Israelin operaatioihin Libanonia ja Hezbollahia kohtaan sekä tämän konfliktin kyberrintaman jatkokehitykseen, ja kyberaseiden käyttöön konfliktien eri vaiheissa ympäri maailman.

Erityisen huomion kohteena taas olivat jatkuvasti lisääntyvät onnistuneet viranomaisoperaatiot kyberrikollisia vastaan, teknologiayhtiöiden puutteelliset yksityiskäytännöt sekä muuttuvat ohjeistukset salasanoihin liittyen. Lokakuulle ja loppuvuodelle seurattavista ilmiöistä haluamme korostaa kvanttisiirtymän aiheuttamia ja edellyttämiä muutoksia sekä Yhdysvaltojen presidentinvaaleihin liittyvän kybervaikuttamisen kiihtymistä.

1. TAPAHTUMIA KYBERMAISEMASSA

Syyskuussa maailmaa hallitsivat uutiset Libanonissa toimivan äärijärjestö Hezbollahin ja Israelin välisen konfliktin leimahtamisesta. Osapuolet ovat käyneet hiljaista sotaa jo vuosikymmenten ajan, mutta syyskuussa Israel kiihdytti tilanteen aktiiviseksi konfliktiksi ensin ilmaiskuilla ja kuun vaihteessa alkaneella maahyökkäyksellä. Jokaisella konfiliktilla on myös oma kyberrintamansa ja informaatioympäristössä käytätävä kilpailu narratiiveista. Yksi tähän konfliktiin liittyvistä eniten huomiota herättäneistä tapahtumista oli Hezbollahin käytössä olleiden hakulaitteiden ja radiopuhelinten räjäytykset. Vaikka kyse ei varsinaisesti ollutkaan kyberhyökkäyksestä, on kybervaikuttaminen osa tämänkin operaation taustavaikuttamia. Syy siihen, miksi Hezbollah alunperin käytti tätä vanhentunutta teknologiaa oli Israelin kyberpelotteessa eli siinä, että järjestön johtoa vaivasi aiheellinen huoli siitä, että Israel pystyy edistynein keinoin vakoilemaan ja seuramaan matkapuhelimia ja niiden välityksellä tapahtuvaa viestintää. Vaikka periaatteessa teknologian tasossa taaksepäin otettu askel voi olla toimiva tapa suojautua kybervaikuttamiselta, tässä tapauksessa se johti huonoihin seurauksiin puutteellisen toimitusketjun turvallisuuden vuoksi.

Konflikti näkyy vahvasti informaatioympäristössä. Israel on pyrkinyt esittämään siviiliuhreja vaatineet ilmaiskunsa ja maahyökkäyksen pakollisena toimenpiteenä, jolla ehkäistään suuremman konfliktin synty. Lisäksi perusteluna käytetään tavoitetta mahdollistaa Israelin pohjoisosista Hezbollahin raketti-iskujen muodostaman uhkan takia evakuoitujen siviilien kotiinpaluu. Tällä on pyritty hakemaan oikeutusta muuten kyseenalaisen aggressiiviselle toiminalle. Kuten aina informaatio-operaatioissa, tavoitteena ei ole koko maailmaan vakuuttaminen vaan tiettyyn yleisöön kohdistuva vaikuttaminen. Israelin todennäköinen tavoite onkin vakuuttaa jo valmiiksi siihen myötämielisesti suhtautuvat valtiot ja muut tahot operaation perusteluista, ja antaa myös näille syy jatkaa tukeaan. Toisaalta Israelin operaatiota on kritisoitu runsaasti useassa länsimaalaisessa mediassa. Etenkin sen aiheuttamaa vahinkoa siviiliväestölle ja välinpitämättömyyttä siviiliuhreista on korostettu. Ajatusta konfliktin ehkäisemisestä aggressiivisella operaatiolla ei myöskään ole nielty, vaan operaation taustalla nähdään tavoite yhden rintaman rauhoittamisesta voimannäytöllä. Päinvastoin tilanteen kiihdyttämisen on arvioitu jopa voivan lisätä koko Lähi-Idän kattavan suursodan todennäköisyyttä.

Ukrainan ja Venäjän välisestä sodasta on opittu, että kyberaseiden käyttö on kiivaimmillaan juuri ennen fyysisen konfliktin alkamista. Perinteisten aseiden puhuessa, muuttuu kybervaikuttamisen rooli taustalla tapahtuvaksi tiedonhankinnaksi ja vastapuolen häirinnäksi. Hezbollahilla ei sinänsä ole ollut varsinaisesti merkittävää osaa kyberrintaman taisteluissa, mutta sen sijaan sitä tukeva Iran on ollut jo vuosia jatkuneessa kyberkonfliktissa Israelin kanssa. Israelin aloitettua operaatiot Hezbollahia vastaan maiden välit ovat entisestään kärjistyneet kybermaailman kamppailusta vuoronperään tehtävien ohjusiskujen tasolle. Ukrainan konfliktissa osapuolet huomasivat melko pian, että kybervaikuttaminen on odotettua huonommin sovellettavissa fyysisen sodan operaatioiden tukemiseen tai tuhovaikutuksen saavuttamiseen. Esimerkiksi kriittiseen infrastruktuuriin kohdistuvat kyberhyökkäykset korvautuivat tähän paremmin soveltuvilla ohjusiskuilla. Ukrainan sodan kontekstissa kyberaseita on alun jälkeen käytetty lähinnä tiedustelun ja informaationhankinnan tukena sekä viime aikoina myös iskuissa huoltoketjuihin. Iranin ja Israelin välillä on kuitenkin yhä pidempi etäisyys kuin Ukrainan ja Venäjän, ja kybervaikuttaminen voi säilyä verrokkitapausta tärkeämpänä työkaluna. Taustalla on varmasti myös Iranin pyrkimus eskalaation välttämiseen, kyberhyökkäykset voidaan toteuttaa niin ettei niiden tekijä paljastu.

2. VALOKEILASSA

2.1. Onnistuneet viranomaisoperaatiot alleviivaavat viestiliikenteen turvallisuuden tärkeyttä

Syyskuussa Europol ja Eurojust yhdessä yhdeksän eri valtion viranomaisten kanssa toteuttivat operaation, jonka seurauksena rikollisten käytössä ollut Ghost-yhteydenpitoalusta ajettiin alas. Lisäksi operaatiossa ympäri maailman pidätettiin 51 henkilöä, takavarikoitiin huumeita ja aseita sekä yli miljoonan euron arvosta käteistä rahaa. Lisäksi suljettiin muun muassa alustaa operoivat palvelimet ja alustaa toiminnassaan käyttänyt huumelaboratorio. Tämä on jatkumoa aiempiin onnistuneisiin viranomaisoperaatioihin, joita länsimaiset viranomaiset yhteistyössä globaalisti ovat toteuttaneet. Kyseessä ollut Ghost-järjestelmä oli vuonna 2015 Australiassa perustettu alusta, jonka keskiössä oli erikoisvalmistettu Ghost-puhelin. Laite oli suunniteltu ja valmistettu nimenomaisesti rikollisten käyttöön, sillä sitä markkinoitiin takuuvarmana tuotteena, jonka viestiliikenteeseen viranomaiset eivät pääsisi käsiksi.

Nyt nähdyn viranomaisoperaation taustalla oli poliisin onnistunut tunkeutuminen alustan toimitusketjuun. Viranomaiset onnistuivat muokkaamaan järjestelmän automaattisia päivityksiä ja sitä kautta saivat alustan haltuunsa käytännössä kokonaan. Tapahtunut alleviivaa viranomaisten kasvavaa kykyä toimia globaalisti yhteistyössä toteuttaen vaativia kyberoperaatioita, joilla on myös välittömät vaikutukset fyysisen maailman rikolliseen toimintaan.

Tapahtunut operaatio herättää varmasti rikollisten piirissä kasvavaa huolta omasta kyberturvallisuudestaan ja toimintansa salassa pysymisestä. Viestiliikenne on usein kyberturvallisuudessa heikko kohta. Niin rikollisilla kuin kaikilla muillakin. Tämä muistuttaa myös meitä yritysmaailmassa, julkisella sektorilla sekä kolmannella sektorilla keskittymään yhä tarkemmin viestiliikenteen kyberturvallisuuteen. Se, missä rikolliset tahot ovat haavoittuvaisimmillaan viranomaistoiminnalle, olemme myös me haavoittuvaisimmillaan rikolliselle toiminnalle. Kussakin organisaatiossa on hyvä pohtia, millä tavalla oma toiminta haavoittuisi, mikäli joku kolmas osapuoli pääsisi organisaation viestiliikenteeseen käsiksi.

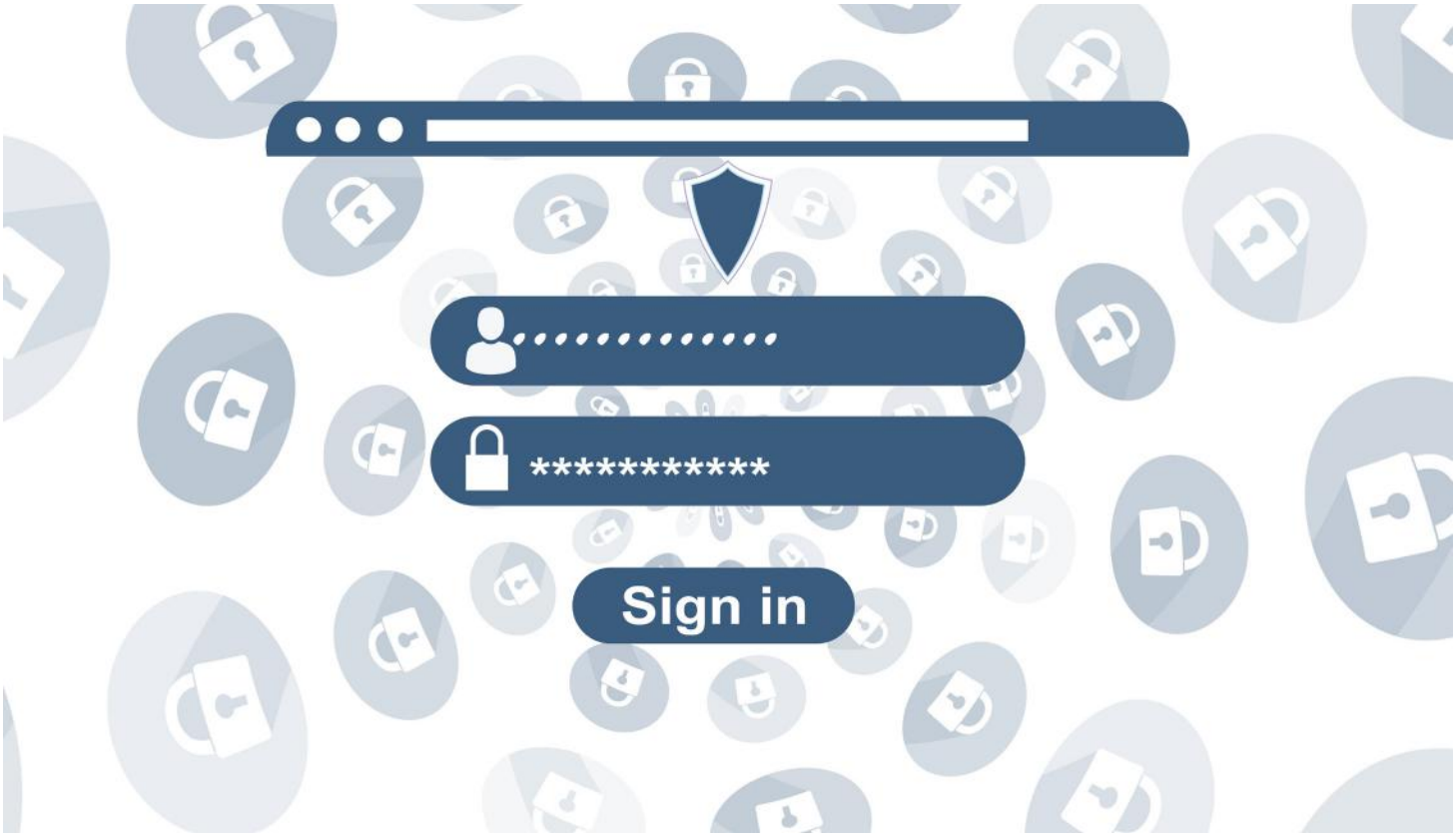
Lähteet sivulla 55

2.2. Teknologiayhtiöt ja sosiaalisen median jätit negatiivisesti esillä syyskuussa

Suuret teknologiayhtiöt sekä sosiaalisen median alustat, kuten Alphabet, Amazon, Apple ja Meta ovat säännöllisesti otsikoissa negatiivisten syiden takia. Syyskuussa Yhdysvaltain paikallinen kuluttajansuojaviranomainen, Yhdysvaltain kauppakomissio (Federal Trade Commission), julkaisi yli neljän vuoden ajan valmistellun raportin sosiaalisen median toimijoiden ja videoalustojen puutteellisista käytännöistä. Tiivistetysti FTC löysi viitteitä muun muassa puutteista palveluiden yksityisyyskäytännöissä, käyttäjien seurannasta sivustolta toiselle, puutteellisesta lasten ja teini-ikäisten suojelusta, käyttäjätietojen jakamisesta kolmansille osapuolille sekä käyttäjätietojen asiattomasta säilyttämisestä. Euroopassa suuret teknologiayhtiöt ovat säännöllisesti saaneet seuraamusmaksuja esimerkiksi yleisen tietosuoja-asetuksen pohjalta. Viimeisimpänä syyskuussa Meta sai Irlannissa 91 miljoonan euron seuraamaksut säilytettyään joidenkin käyttäjien salasanoja suojattomasti selkotekstinä järjestelmissään. Tietosuoja-asioiden lisäksi teknologiayhtiöt ovat Euroopassa olleet syyskuussa otsikoissa Applen veroepäselvyyksien sekä Googlen epäiltyjen kilpailulainsäädäntörikkomusten vuoksi.

Suuryritysten vaikeudet sovittaa omat toimensa lainsäädännön tai hyvien käytänteihin rajoihin ovatkin silmiinpistäviä Atlantin molemmilla puolilla ja ne ovat saaneet paljon kritiikkiä myös muista syistä. Villeimmissä väitteissä sosiaalisen median yhtiöiden ja teknologiayhtiöiden on arveltu jopa luovan uhkan demokratialle. Tästä esimerkkinä toimivat alustoilla leviävät valeuutiset, vihapuhe ja sekä syvävääränrennökset, joilla arvellaan voivan olla vaikutuksia vaalituloksiin demokraattisissa valtioissa. Edelleen niiden koukuttavuuden on nähty vaikuttavan erityisesti lapsiin ja nuoriin. Kauniista vastuullisuuspuheista huolimatta teknologia- ja alustajätit vaikuttavat olleen suhteellisen haluttomia puuttumaan kritiikkiin tai nostettuihin ongelmakohtiin tosissaan. Tästä kielivät myös jatkuvat seuraamusmaksut – mieluummin toimitaan lakeja rikkoen ja myöhemmin tarvittaessa maksetaan langetetut korvaukset.

Lienee selvää, että teknologiayhtiöiden ja sosiaalisen median palveluiden toiminnan valvomiseen olisi keksittävä uusia keinoja. Tästä voisi sanoa vallitsevan jopa jonkinlaisen konseksuksen kansalaisyhteiskunnan ja poliittisten päättäjien kesken. Syyskuun perusteella uusia toimenpiteitä teknologiajättien suitsimiseen tuskin on tulossa. FTC suositteli raportissaan seuraavia muun muassa datan keräyksen hillitsemistä sekä seurantateknologioista luopumista, mutta niiden ollessa vain suosituksia, on todennäköistä, että ne kaikuvat kuuroille korville. Globaaliongelma kaipaisi kuitenkin globaaleja ratkaisuja. Esimerkiksi EU:n ja Yhdysvaltain viranomaisten välinen yhteistyö, lainsäädännön harmonisointi sekä teknologiayhtiöiden vastuiden määrittely ja tarkempi seuranta voisivat toimia keinoina ongelmaan vastaamiseksi. Tavallisten käyttäjienkin tulisi herätä ongelmaan. Mikäli yksilöt itse eivät ole kiinnostuneita omasta datastaan tai oikeuksistaan, voidaanko sitä edellyttää taloudellisten lainalaisuuksien perusteella toimivilta suuryrityksiltäkään?



2.3. Salasanakäytännöt muuttuvat

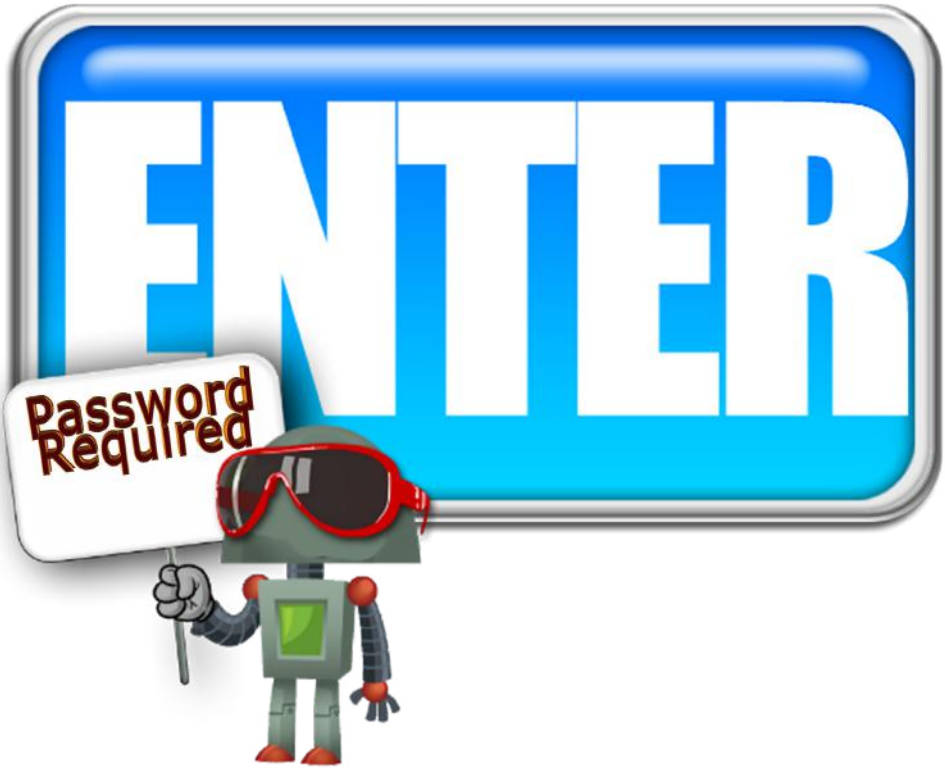
Salasanat ovat pitkään käytössä ollut, mutta puutteelliseksi havaittu tunnistautumissmenetelmä. Niitä usein kuvataan huonona, mutta parhaana käytössä olevana tunnistautumisvaihtoehtona. Vaikka korvaavia ratkaisuja kehitetään jatkuvasti, ovat salasanat ainakin vielä ylivoimaisesti eniten käytetty ratkaisu. Salasanoihin liittyvät ongelmat eivät keskity itse teknologiaan sinänsä, vaan ihmisiin niiden käyttäjinä. Niiden heikkoudet kumpuavat heikoista, uudelleen käytetyistä, unohdetuista tai kadotetuista salasanoista. Salasanojen turvallisuutta pyritään lähes jokaisessa käyttökohteessa parantamaan määrittämällä minkälainen salasanan tulee olla. Usein organisaatioilla on ohjeistuksia tai vaatimuksia liittyen salasanojen ainutlaatuisuuteen tai ylläpidettäviä kiellettyjen sanojen listauksia. Ihmiset ovat kuitenkin huonoja noudattamaan ohjeita, etenkin mikäli ne tuntuvat hankalilta. Tästä syystä salasanojen käyttöön liittyvät ohjeistukset joutuvat tasapainottelemaan eturvallisuuden ja helppokäyttöisyyden välillä.

Kuun vaihteessa salasanoihin liittyvää ohjeistusta on jälleen pyritty kehittämään, tällä kertaa Yhdysvaltain standardisointi- ja teknologiainstituutti NIST:n (National Institute of Standards and Technology) toimesta. Virasto on julkaissut uuden ohjeistuksen liittyen siihen, minkälaiset salasanat ja niihin liittyvät käytännöt ovat sen mukaan turvallisia, ja miten käyttäjiä tulisi ohjeistaa ja valvoa niiden käytössä. NIST:n ohjeistus otetaan suoraan käyttöön ainakin suuressa osassa Yhdysvaltojen hallinto- ja viranomaiaorganisaatioissa ja sen odotetaan toimivan myös ohjenuorana yksityisten yritysten tai organisaation käytänteisiin. Tärkeimpiä ja mielenkiintoisimpia nostoja ohjeistuksesta ovat painotuksen siirtyminen monimutkaisista salasanoista yksinkertaisempiin mutta pidempiin salasanoihin, sekä ajastetuista tai pakotetuista salasanavaihdoksista luopuminen.

Ensimmäisellä näistä tarkoitetaan sitä, että ohjeistuksia siihen minkälaisia merkkejä salasanojen tulee sisältää yksinkertaistetaan ja suoraviivaistetaan. Kelle tahansa uutta palvelua rekisteröineelle on varmasti tuttua, että palvelu ei kelpuuta ensin tarjottua salasanaa vaan vaatii, että sen tulee sisältää esimerkiksi sekä isoja että pieniä kirjaimia, numeroja ja erikoismerkkejä. NIST:n mukaan tämänkaltaiset vaatimukset eivät todellisuudessa merkittävästi lisää salasanojen turvallisuutta, vaan enemmänkin päinvastoin. Ne johtavat huonoihin salasanakäytänteisiin kuten samojen tai kaavamaisten salasanojen käyttöön eri järjestelmissä, unohduksiin tai salasanojen jakamiseen ja vain äärimmäisen harvoin niiden avulla saavutetaan tavoiteltu lisäturva salasanoihin kohdistuviin arvaus- tai murtohyökkäyksiin liittyen.

Teoriassa erilaisten merkkien sisällyttäminen salasanaan lisää salasanan kestävyyttä esimerkiksi väsytyshyökkäystä kohtaan eksponentiaalisesti, mutta käytännössä tämä toteutuu vain harvoin. Yleensä salasanoissa erikoismerkit ja numerot eivät ole satunnaisesti mukana salasanan keskellä vaan lähes aina joko alussa tai lopussa, jolloin tavoiteltu monimutkaisuus ei todellisuudessa toteudu. Väsytyshyökkäyksiä huomattavasti yleisempää on salasanojen murtaminen arvaamalla tai

Lähteet sivulla 55



hyödyntämällä yleisesti käytettyjä tai saman käyttäjän muita salasanoja. NIST:n ohjeistus pyrkiikin muokkaamaan käytänteitä siihen suuntaan, että käyttäjät muistaisivat salasanansa helpommin, ja suosimaan sanojen sisään salalauseita. Useasta sanasta koostuvia lauseita on vaikeampi arvata ja helpompi muistaa etenkin, kun niihin ei tarvitse sotkea erikoismerkkejä tai numeroita. Toki ohjeistuksessa yhä sallitaan kaikkien eri merkkityyppien käyttö, ja sallittuja merkkityyppejä jopa kehotetaan lisäämään, mutta niiden käyttö ei enää ole pakollista salasanaa luodessa. Vaatimuksena enää tulisi olla vain vähintään kahdeksan merkkiä pitkä salasana, mutta jopa 64 merkin pituiset salalauseet tulisi sallia.

NIST myös kehottaa organisaatiota luopumaan pakotetuista ajastetuista salasananvaihdoksista. Salasanojen pakotettu vaihtaminen tulisi olla keino, jota käytetään vain mikäli on epäilys tai tieto siitä, että tunnukset ovat paljastuneet esimerkiksi tietomurrossa tai niihin liittyy epäilyttävää toimintaa. Esimerkiksi muutaman kuukauden välein pakotettu salasanan vaihto ei lisää turvallisuutta, vaan samoin kuin monimutkaiset vaatimukset, vain lisäävät todennäköisyyttä turvallisuutta heikentäviin toimintamalleihin. Näiden ohjeistuksien lisäksi NIST kehottaa luopumaan salasanavinkeistä, tai niiden palauttamisen mahdollistavista turvallisuuskysymyksistä, sillä nämäkin voivat olla helppoja arvata ja pahimmillaan helpompi keino murtautua järjestelmiin kuin itse salasanojen urkinta.

NIST siis vaikuttaa jakavan monien asiantuntijoiden käsityksen siitä, että mitä monimutkaisemmat vaatimukset salasanoille on, tai mitä useammin niitä joutuu keksimään uusia sitä todennäköisempää on, että käytössä olevat salasanat ovat jollain tavalla huonoja. Ajatukset pidempien salalauseiden suosimisesta monimutkaisten lyhyiden salasanojen sijaan tai pakotetuista vaihdoksista luopuminen eivät ole sille uniikkeja ajatuksia, vaan monen muunkin tahon esiin nostamia parannusehdotuksia salasanoihin liittyen. NIST kuitenkin toteaa, että kyseessä on joka tapauksessa heikko, ja väärinkäytöksille ja hyökkäyksille altis ratkaisu, jota tulisikin aina kuin mahdollista tukea tai korvata esimerkiksi biometrisellä tai monivaiheisella tunnistautumisella. NIST ei suoraan suosittele erilaisten salasananhallintaohjelmistojen käyttöä, vaikka yleisesti näitä pidetään verrattain toimivana tapana tuottaa ja ylläpitää uniikkeja ja kestäviä salasanoja. Syy siihen, että NIST ei tätä vaihtoehtoa suosittele liittyykin ratkaisujen huonouden sijaan todennäköisesti enemmän siihen, että niiden käyttö edellyttää auditointia ja luottamusta palveluntarjoajaa kohtaan. Salasananhallintaohjelmistot ovat luonnostaan hyvin houkuttelevia kohteita kyberhyökkäyksille, ja NIST ei voi suositella yleisesti minkä tahansa tuottajan ratkaisun käyttämistä, sillä niiden turvallisuudessa on havaittu merkittäviä eroja.

Joka tapauksessa sekä arkipäiväisten käyttäjien että organisaation salasanakäytänteistä vastaavien tulisi harkita sitä, minkälaiset salasanat tai niihin liittyvät vaatimukset todellisuudessa edistävät turvallisuutta, ja mitkä eivät. NIST:n ohjeistus voi toimia hyvänä lähtökohtana salasanakäytännön päivittämiseen. Käytäntöjen lisäksi kriittistä on lisäksi hankkia näkyvyyttä ja havainnointikykyä jo mahdollisesti vuotaneista salasanoista, sillä monimutkaisin tai pisinkään salasana ei ole juuri 1234:ää turvallisempi, jos se löytyy pimeästä verkosta käyttäjätunnukseen liitettynä.

NIST suositukset löytyvät kokonaisuudessaan täältä: https://pages.nist.gov/800-63-4/sp800-63b.html

3. SEURAA NÄITÄ

3.1. Yhdysvaltojen presidentinvaalien lähestyessä vaalivaikuttaminen kiihtyy

Yhdysvaltojen vaalit ovat tänä vuonna, kuten aiemminkin, olleet merkittävän huomion kohteena kybermaailmassa. Erilaisia vaikuttamisoperaatiota on jo nähty ja tullaan ennen vaaleja näkemään lisää. Pääosin vaikuttamisyritykset ovat olleet erilaisia informaatio-operaatioita, joilla pyritään vaikuttamaan näkemyksiin kandidaateista sekä heidän ajamistaan poliittisista agendoista. Kohdistetut kyberhyökkäykset ehdokkaita tai heidän kampanjatiimejään kohtaan ovat harvalukuisempia. Niitäkin on silti jo nähty, ja pyrkimykset ovat olleet esimerkiksi hakkeroida merkittävien henkilöiden sähköpostitilejä sekä muita tilejä, ja julkaista niiden sisältämiä viestejä. Myös vaalien verkkosivuille on kohdistettu hajautettuja palvelunestohyökkäyksiä (DDoS). Näiden tavoitteena on ollut häiritä vaaleja ja hankaloittaa tiedon saamista. Iskut eivät kuitenkaan ole lopulta häirinneet vaalien turvallista toteutumista.

Näkyvin vaaleihin liittyvä kyberoperaatio tapahtui elokuussa, kun republikaanien presidenttiehdokkaan Trumpin kampanja ilmoitti olleensa kyberhyökkäyksen kohteena. Tuolloin hyökkäyksessä ulkopuolinen taho oli päässyt Trumpin lähipiirissä olevan poliitikon sähköpostiviesteihin käsiksi. Tämän jälkeen hyökkääjä lähetti kaapattuja sähköpostiviestejä yhdysvaltalaisille mediataloille, jotka kuitenkin kieltäytyivät niitä julkaisemasta. Tapahtuneesta on nostettu syytteet kolmelle Iranin islamilaisen vallankumouskaartin jäsenelle. Hyökkäys toteutettiin kohdennetulla kalasteluhyökkäyksellä.

Yhdysvaltain viranomaiset ovat lisäksi ilmoittaneet lukuisista valeuutissivustojen alasajoista sekä erilaisista valeuutiskampanjoista. Viranomaisten mukaan suurin yksittäinen lähde valeuutisten takana on Venäjän valtio ja etenkin sen mediayhtiöt, kuten Russia Today (RT) ja siihen kytköksissä olevat toimijat. Venäjää on syytetty muun muassa tekoälyn, bottiverkostojen sekä valeuutissivustojen käytöstä oman propagandansa levittämiseen. Venäjän lisäksi valeuutisia sekä dis- ja misinformaatiota Yhdysvaltojen presidentinvaaleihin liittyen levittää moni muu valtiotasoinen toimija, kuten Kiina ja Iran. Myös Yhdysvaltojen sisäiset toimijat levittävät tahattomasti tai tahallisesti erilaisia valeuutisia sekä väärää tietoa vaalien kontekstissa.

Viranomaiset ovat ottaneet päättäväisesti kantaa erilaisiin vaikuttamisoperaatioihin ja informaatiokampanjoihin. Tavoitteena on välttää vuoden 2016 vaalien kaltaiset tapahtumat, jolloin muun muassa Venäjän todettiin levittäneen runsaasti erilaista mis- ja disinformaatiota vaaleihin liittyen. Tällöin viranomaisten varoitukset ja ohjeistukset eivät kerenneet kunnolla tavoittaa äänestäjiä ennen vaalipäivää. Nyt viranomaiset ovat lähteneet ajoissa kampittamaan kaikenlaisia informaatiokampanjoita, joiden totuusperälle ei ole näyttöjä. Demokratiassa kuitenkin väärän tiedon kitkemisen ja sensuurin tason määrittely on erittäin vaikeaa. Missä määrin väärää tietoa tai harhaan johtavaa tietoa on oikein poistaa verkosta, ajatellen sananvapautta ja mielipiteen ilmaisemisen oikeutta. Tämä tasapainoilu on erittäin haastavaa ja sitä onkin hyvä arvioida seuratessa Yhdysvaltojen presidentinvaaleja ja sen yhteydessä käytävää poliittista keskustelua.

Yhdysvaltojen ollessa yksi merkittävimmistä ja suurimmista demokratioista, seurataan sen vaaleja tarkasti ympäri maailmaa. Näiden vaalien yhteydessä käytävä informaatio- ja kybertaistelu näyttäytyy koko maailmalle esimerkkinä siitä, mitä kaikkea vaalien yhteydessä ollaan valmiita tekemään. Etenkin autoritaaristen valtioiden tavoitteena on ylipäänsä luoda epäluottamusta demokraattiseen järjestelmään sekä luoda kansojen sisälle voimakasta eripuraa ja polarisaatiota. Informaatiovaikuttamiselta pystytään välttymään varsin hyvin medianlukutaidolla eli suhtautumalla kriittisesti verkkosisältöihin. Lisäksi virheellinen tieto tai esimerkiksi valeuutissivustot on hyvä ilmoittaa viranomaisille tai sivustojen ylläpitäjille, jotka sitten pyrkivät katkaisemaan tämän väärän tiedon leviämistä.

Lähteet sivulla 55

3.2. Kvanttisuojatut standardit ovat valmiita ja implementointi voi alkaa

Kvanttitietokoneiden muodostamasta uhkasta on oltu tietoisia ja huolissaan jo vuosikymmenten ajan. Käytännössä huoli liittyy siihen, että kun tarpeeksi tehokas kvanttikone muuttuu teoriasta todeksi, voi sen laskentatehon avulla murtaa kaiken nykyisin käytössä olevan salausteknologian. On vain ajan kysymys, milloin tämä tapahtuu. Asiantuntijoiden arviot vaihtelevat vuosista vuosikymmeniin. Koska uhka on sekä vakava että tiedostettu, on siihen pyritty valmistautumaan jo pidemmän aikaa. Ratkaisuna pidetään uudenlaisia salausalgoritmeja, jotka toisin kuin nykyisin käytössä olevat, kestäisivät myös tulevaisuuden kvanttitietokoneen hyökkäyksen. Salausalgoritmit ovat monimutkaisia matemaattisia prosesseja, joilla tietojärjestelmään tallennettu tai niiden välillä siirtyvä data tehdään lukukelvottomaksi ilman oikeanlaisia purkuavaimia. Näin tieto salataan ulkopuolisilta. Uusien algoritmien kehittäminen on hidasta, ja niihin siirtyminen on pitkä monivuotinen prosessi. Kvanttiuhkaan varautuminen onkin tähän mennessä rajoittunut lähinnä uhkan tiedostamiseen sekä keskusteluksi ja pohdinnaksi siitä, minkälaiset algoritmit olisivat parhaita kvanttiuhkaan vastaamiseksi.

Yksi eniten konkreettisia asioita kvanttisiirtymää varten tehnyt taho on Yhdysvaltain standardisointi- ja teknologiainstituutti NIST (National Institute of Standards and Technology). Noin kahdeksan vuoden ajan jatkuneessa prosessissa NIST on kerännyt, testannut ja parannellut sille tehtyjä esityksiä potentiaalisista kvanttikestävistä salausalgoritmeista tavoitteenaan tuottaa standardit, joiden mukaan tietojärjestelmät voitaisiin tulevaisuudessa turvata. Nyt alkusyksystä ensimmäiset näistä on julkaistu standardien FIPS 203, FIPS 204 ja FIPS 205 muodossa. NIST:n työn valmistumista on odotettu ympäri maailman ja sen myötä ensimmäiset käytännön askeleet kvanttisiirtymää varten voidaankin ottaa. Siirtymä ei kuitenkaan tule olemaan hetkessä ohi. Vaikka aikaa uhkan realisoitumiseen onkin vielä vuosia, NIST on kehottanut aloittamaan prosessin jo nyt. Joitain kvanttikestäviä ratkaisuja on jo olemassa, lähinnä yksityisten toimijoiden kuten Googlen, Amazonin ja Applen omiin tuotteisiinsa implementoimina. Laajamittaisesta siirtymästä vastaavat viranomaiset tai regulaattorit, kuten Euroopassa ENISA, ovat odottaneet NIST:n standardeja. Nämä ovat kaupallisia verrokkeja enemmän testattuja ja suunniteltu yhteensopiviksi nyt käytössä olevien ratkaisujen kanssa, minkä lisäksi yhdenmukainen standardoitu ratkaisu on myös tulevaisuuden kannalta tarpeellinen.

Ongelmatonta siirtymästä ei kuitenkaan odoteta. Vaikka pohjatyö on tehty huolella, kyse on silti vielä pitkälti vain teoriassa testatuista ratkaisusta. On todennäköistä, että standardeista tulee löytymään aukkoja tai yhteensovittamisessa nousee ennakoimattomia haasteita. Myös NIST tiedostaa haasteet ja on varautunut niihin ilmoittamalla julkaisevansa vielä loppuvuodesta ja ensi vuonna uusia standardeja. Näiden on tarkoitus toimia varalla, mikäli nyt julkaistut murretaan tai osoittautuvat muuten puutteellisiksi. NIST:n mukaan varastandardeja ei kuitenkaan tule eikä kannata odottaa vaan toimenpiteet nyt julkaistujen käyttöönottamiseksi tulee aloittaa välittömästi.

Ketä kehotus kvanttisiirtymän aloittamiseksi nyt siis koskee ja mitä kvanttisiirtymä tulee edellyttämään? Pienten ja keskisuurien toimijoiden ei tarvitse huolestua, sillä näiden kohdalla muutos tulee näkymään lähinnä siinä, että jossain kohtaa käytössä olevat järjestelmät ja ratkaisut tulevat lähivuosina päivittymään kvanttisuojatuiksi. Päättäjien, lainsäätäjien ja omia ratkaisujaan tuottavien on kuitenkin syytä pysyä kärryillä tilanteen kehittymisestä. Suurempien organisaatioiden on syytä aloittaa työ kaiken suojattavan datan kartoittamiseksi ja massiivisen muutoksen suunnittelemiseksi. Euroopassa organisaatioiden on muutenkin syytä tarkastella salauskäytäntöjään, sillä niihin liittyy velvoitteita NIS2-direktiivin muodossa. ■

LÄHTEET

TAPAHTUMIA KYBERMAISEMASSA

Cyberwatchin viikkokatsaukset syyskuulta
https://www.aljazeera.com/news/2024/9/24/why-is-israel-attacking-lebanon
https://www.csis.org/analysis/escalating-war-between-israel-hezbollah-and-iran

ONNISTUNEET VIRANOMAISOPERAATIOT ALLEVIIVAAVAT VIESTILIIKENTEEN TURVALLISUUDEN TÄRKEYTTÄ

https://www.reuters.com/technology/cybersecurity/ghost-cybercrime-platform-dismantled-global-operation-51-arrested-2024-09-18/
https://www.europol.europa.eu/media-press/newsroom/news/global-coalition-takes-down-new-criminal-communication-platform
https://www.theregister.com/2024/09/18/51_arrests_ghost_platform/

TEKNOLOGIAYHTIÖT JA SOSIAALISEN MEDIAN JÄTIT NEGATIIVISESTI ESILLÄ SYYSKUUSSA

https://therecord.media/meta-unprotected-passwords-fine-gdpr
https://www.reuters.com/technology/eu-privacy-regulator-fines-meta-91-million-euros-over-password-storage-2024-09-27/
https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance
https://www.cnbc.com/2024/09/10/apple-loses-eu-court-battle-over-13-billion-euro-tax-bill-in-ireland.html
https://www.theregister.com/2024/09/19/social_media_data_harvesting_handling_ftc/

SALASANAKÄYTÄNNÖT MUUTTUVAT

https://www.darkreading.com/identity-access-management-security/nist-drops-password-complexity-mandatory-reset-rules
https://pages.nist.gov/800-63-4/sp800-63b.html
https://www.hivesystems.com/blog/are-your-passwords-in-the-green

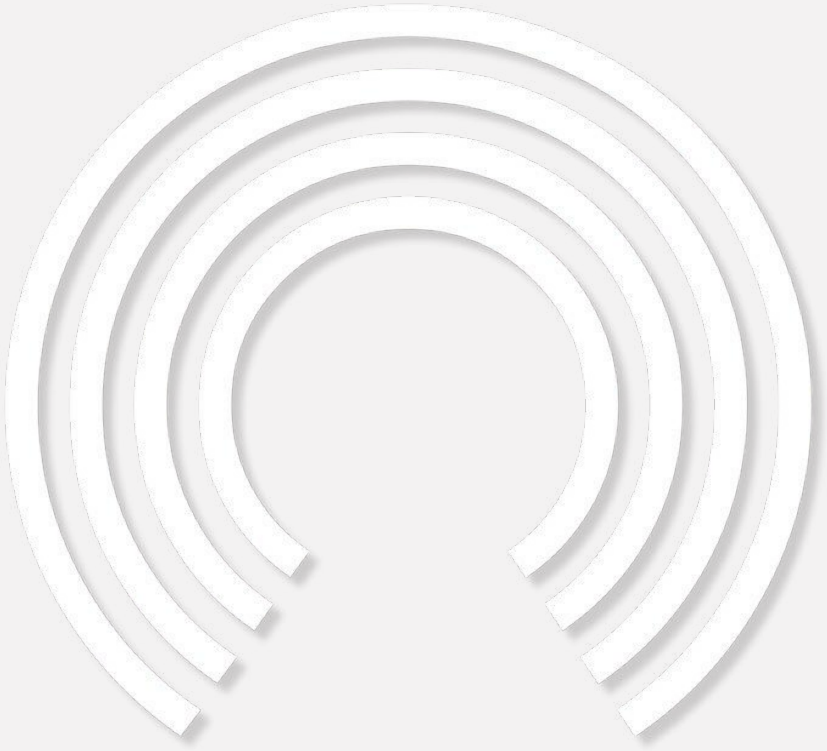
YHDYSVALTOJEN PRESIDENTINVAALIEN LÄHESTYESSÄ VAALIVAIKUTTAMINEN KIIHTYY

https://www.nytimes.com/2024/09/04/us/politics/russia-election-influence.html?unlocked_article_code=1.PE4.B1C6.ZXLPVBRImUyl&smid=url-share
https://www.nbcnews.com/news/investigations/us-garland-indicts-three-iranians-trump-campaign-hack-rcna173001
https://www.state.gov/united-states-sanctions-iran-backed-malicious-cyber-actors-that-have-attempted-to-influence-u-s-elections/
https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3994-odni-pr-22?
https://www.brookings.edu/articles/foreign-influence-operations-in-the-2024-elections/
https://www.cisa.gov/news-events/news/cisa-and-fbi-release-joint-psa-putting-potential-ddos-attacks-during-2024-election-cycle-context

KVANTTISUOJATUT STANDARDIT OVAT VALMIITA JA IMPLEMENTOINTI VOI ALKAA

https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
https://www.technologyreview.com/2022/09/14/1059400/explainer-quantum-resistant-algorithms/
https://www.bleepingcomputer.com/news/security/nist-releases-first-encryption-tools-to-resist-quantum-computing/

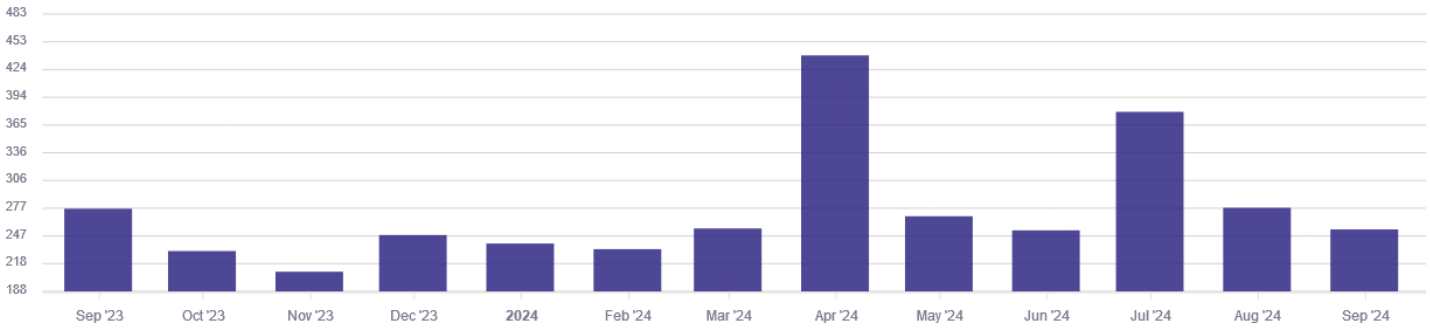
Cyberwatch Finland



UHKATIEDUSTELUSEURANTA

Cyberwatch Finland julkaisee uhkatiedusteluseurannan, johon on koottu viimeisen kuukauden ajalta merkittävimpiä kyberhyökkäyksiä sekä tietoa aktiivisimmista ja nousevista uhkatoimijoista ympäri maailmaa. Cyberwatchin analyytikot seuraavat paitsi pintaverkossa, myös syvässä ja pimeässä verkossa tapahtuvaa toimintaa. Lähteenä on lisäksi kansainvälisten tietoturvatoimijoiden julkaisuja sekä laaja suomalaisen ja kansainvälisen mediakentän seuranta

TIETOVUODOT KUUKAUSITTAIN VIIMEISEN VUODEN AJALTA.



Lähde: Cyber Intelligence House

MERKITTÄVIMPIÄ KYBERISKUJA JA -KAMPANJOIA

HOLLANNIN POLIISI

AJANKOHTA: Tapahtumasta ilmoitettu 27.09.2024
KUVAUS: Syyskuun lopulla Alankomaiden poliisi ilmoitti joutuneensa kyberhyökkäyksen kohteeksi. Poliisi ilmoitti, että sen henkilöstöä koskevat tietokannat olivat hyökkääjän kohteina ja näistä sen onnistui varastaa määrittelemättömän määrän poliisien henkilötietoja. Myöhemmin hyökkäyksen taustalla ilmoitettiin olevan valtiollinen toimija, mutta tarkempia syytöksiä mitään tiettyä tahoa kohteen ei ole tehty. Mikään tunnettu hakkeriryhmä ei ole ilmoittanut olevansa iskun takana. Aiemmin Alankomaiden viranomaiset ovat ilmaisseet huolensa etenkin kiinalaisten ja venäläisten uhkatoimijoiden operaatioista maata kohtaan.
TEKIJÄ: Ei tiedossa / valtiollinen toimija
MOTIIVI: Ei tiedossa
VAIKUTUKSET: Alankomaiden poliisien tietoja, kuten nimiä, sähköpostiosoitteita, puhelinnumeroita ja joissain tapauksissa myös muita henkilötietoja päätyi hyökkääjän tietoon. Tietoja ei ole ilmestynyt myyntiin tai jakoon, joten on epäselvää mitä tarkoitusta varten tietomurto tehtiin.

MERKITTÄVIMPIÄ KYBERISKUJA JA -KAMPANJOIA

ALISA PANKKI JA TYTÄRYHTIÖ MOBIFY INVOICE

AJANKOHTA: 03.10.2024
KUVAUS: Alisa pankin tytäryhtiön Mobify Invoicen asiakastiedote sisälsi virheellisesti koko yhtiön asiakaskannan sähköpostiosoitteet. Tuhansille pankin asiakkaille lähtenyt viesti sisälsi koko lähetyslistan osoitteet. Asiaa pahoiteltiin ja perusteltiin inhimillisellä virheellä.
TEKIJÄ: Sisäpiiriläinen
MOTIIVI: Inhimillinen erehdys
VAIKUTUKSET: Sähköpostiosoitteiden paljastuminen sinällään ei muodosta merkittävää uhkaa, mutta koko asiakaslistan vuotaminen voi olla hyödyllistä esimerkiksi pankin nimissä huijauksia tehtaileville rikollisille. Lisäksi tapahtuma on pankin kannalta nolo ja vaikuttaa varmasti asiakasluottamukseen. Mainehaitan suuruus paljastuu vasta myöhemmin, riippuen asiakkaiden reaktioista.

TIETOTURVAYHTIÖ CLOUDFLAREN HAVAITSEMA ENNÄTYSTEHOKAS DDOS-HYÖKKÄYS

AJANKOHTA: Syyskuu 2024
KUVAUS: Tietoturvayhtiö Cloudflare ilmoitti syyskuussa havainneensa ja onnistuneesti torjuneensa asiakkaidensa kohtaaman, ennätystehokkaaksi mainostetun, hajautetun palvelunestohyökkäyksen, eli niin kutsutun DDoS-hyökkäyksen. Hyökkäyksen maksimiteho oli 3,8 terabittia sekunnissa (Tbps) ja 2,14 miljardia pakettia sekunnissa (Pps).
TEKIJÄ: Tuntematon
MOTIIVI: Hyökkäyksen tarkasta motiivista ei ole tietoa, mutta Cloudflaren mukaan hyökkäys kohdistettiin muun muassa finanssi-, internet- ja mobiiliverkkopalveluita tarjoaviin organisaatioihin.
VAIKUTUKSET: Vaikka Cloudflaren eräänä motiivina raportoida tapauksesta on markkinoida ja myydä omia suojauspalveluitaan, tapaus todistaa sen, että palvelunestohyökkäyksiltä voidaan tarvittaessa suojautua. Palvelunestohyökkäykset ovat yleinen kyberuhka, jota esimerkiksi venäläiset haktivistiryhmät ovat usein käyttäneet.

VERKKOKAUPPAJÄTTI TEMUN TIETOMURTO

AJANKOHTA: 17.9.2024
KUVAUS: Muutoinkin laajan yhteiskunnallisen keskustelun kohteena oleva kiinalainen verkkokauppatoimija Temu joutui mahdollisen tietomurron kohteeksi syyskuussa. BreachForums-hakkerifoorumille ilmestyi myynti-ilmoitus, jossa ilmoittaja ilmoitti kauppaavansa yli 87 miljoonaan tietueen pakettia, joka sisältää muun muassa verkkokaupan asiakastietoja.
TEKIJÄ: Tietoja kauppaava hakkeri tai hakkeriryhmä esiintyy nimimerkillä smokinthashit.
MOTIIVI: Taloudellinen
VAIKUTUKSET: Temu kiistää joutuneensa tietomurron uhriksi ja on uhannut oikeusjutuilla “misinformaatiota” levittäviä tahoja. Yhtiö ilmoitti tarkastaneensa hakkereiden julkaisemia näytekappaleita vuotaneista tiedoista ja kertoi, että ne eivät vastaa yhtiön hallussa olevaa dataa. Vastaavasti uhkatoimija vakuuttaa tietojen olevan aitoja. Kummankaan osapuolen esittämiä väitteitä ei voida luotettavasti tarkistaa. Tapaus joka tapauksessa korostaa verkkokauppoihin ja niistä tilaamiseen liittyviä riskejä, mikä voi johtaa henkilötietojen vuotamiseen pimeille markkinoille, mikäli tietoturva on heikosti toteutettu.

AKTIIVISIMPIA SEKÄ NOUSEVIA UHKATOIMIJOITA

RANSOMHUB

KUVAUS: Tammikuussa 2024 ilmestynyt lunnashaittaohjelmatoimija, joka toimii RaaS–palveluntarjoajana. Ryhmä ottaa alihankkijoiltaan 30 % provision kaikista lunnastuloista. Ryhmän toimintaa on jäljitetty useisiin eri maihin, kuten Kiinaan, Pohjois-Koreaan, Kuubaan, Romaniaan sekä useisiin CIS maihin. Ryhmä kohdistaa vihamieliset aktiviteettinsa muihin kuin edellä mainittuihin maihin.
VIIME AIKOJEN TOIMINTA: Aktiivisuus kasvanut tasaisesti alkuvuoden aikana ja ryhmä olikin menneen kuun aktiivisin ilmoittamillaan 75 uhrilla. Viimeisimpiä ryhmän uhreja ovat muun muassa keittiötarvikkeita myyvä Domain Industries –yritys sekä apuvälineitä tarjoava Rollx Vans.
TOIMINTATAVAT JA TAKTIIKAT: Käyttää niin tiedon tuhoamis- kuin myös salaustekniikoita hyökkäyksissään. Haittaohjelmakoodit ovat Golang ja C++ pohjaisia. Ryhmän haittaohjelmakoodi toimii Windows, LINUX ja ESXi pohjilla.

CACTUS

KUVAUS: Kiristyshaittaohjelmatoimija, joka on ollut aktiivinen ainakin vuoden 2023 maaliskuusta lähtien.
VIIME AIKOJEN TOIMINTA: Ryhmä oli kuluneen kuun toiseksi aktiivisin uhkatoimija ilmoittamillaan 26 uhrilla.
TOIMINTATAVAT JA TAKTIIKAT: Ryhmä hyödyntää ostettuja tunnistetietoja, kumppanuuksia eri haittaohjelmatoimijoiden kanssa, tietojenkalasteluhyökkäyksiä ja tietoturva-aukkoja. Ryhmä on hyödyntänyt muun muassa VPN-ohjelmien haavoittuvuuksia. Ryhmä toteuttaa toiminnassaan kaksoiskiristystä, eli lunnaiden maksamattajättämisen seurauksena uhrin tiedot laitetaan myyntiin tai julkaistaan ilmaiseksi verkkoon.

NITROGEN RANSOMWARE

KUVAUS: Kesällä 2024 havaittu uusi kiristyshaittaohjelmatoimija. Ryhmän uhreina on etenkin IT alan sekä kolmannen sektorin organisaatioita Yhdysvalloissa.
VIIME AIKOJEN TOIMINTA: Ryhmän uhreina on viime aikoina ollut muun muassa peliyhtiö Kanadasta, insinööritoimisto Yhdysvalloista sekä raskaskaluston leasing palvelu Yhdysvalloista
TOIMINTATAVAT JA TAKTIIKAT: Toiminta perustuu Google ja Bing mainoksiin upotettuihin haittaohjelmiin. Uhri houkutellaan lataamaan kyseinen haittaohjelma, jonka jälkeen hyökkääjä tunkeutuu uhrin tietoverkkoihin ja tämän jälkeen suorittaa erilaisia tietovarkauksia, kybervakoilua ja kiristyshaittaohjelma-hyökkäyksiä.

HANDALA HACK TEAM

KUVAUS: Iranilainen maan vallankumouskaartiin yhdistetty uhkatoimija. Pidetään yhtenä Iranin tehokkaimmista hakkeriryhmistä, jonka kohteena usein Israel. Ryhmä aktivoitunut vuoden 2023 joulukuussa ja ylläpitää useita sosiaalisen median tuen keräys- ja viestintäkanavia. Ilmoittanut tukevansa Hamasia konfliktissa Isrealia vastaan.
VIIME AIKOJEN TOIMINTA: Viime aikoina moninkertaistanut iskunsa Israelia ja etenkin maan puolustus- ja sotilasteollisuutta kohtaan. Syyskuun lopulla ryhmä ilmoitti iskeneensä israelilaiseen ydinvoimatutkimuslaitokseen varastaen noin 200 gigatavun edestä dataa. Iskua ei ole vahvistettu viranomaisten toimesta. Ryhmä itse ilmoitti iskun toteuttamisesta ja sen oletetaan olevan kosto Hezbollah johtaja Hassan Nasrallahin murhasta Libanonissa.
TOIMINTATAVAT JA TAKTIIKAT: Ryhmä toteuttaa korkeasti edistyneitä ja toimintatavaltaan vaihtelevia iskuja Israelin hallintoa ja maan yrityksiä kohtaan. Iskujen tavoitteena ei ole taloudellinen hyöty, vaan ryhmä usein julkaisee kaappaamansa datan ilmaiseksi. Ryhmän on todettu myös liioitelleen iskujaan ja joskus jopa ilmoittaneen täysin valheellisia kyberhyökkäyksiä. Tavoitteena on vaikuttaa Israelin kykyyn käydä sotaa ja psykologinen vaikuttaminen väestöön.

INTOHIMONA KYBERTURVALLISEMPI MAAILMA

Cyberwatch Finland on strategisen kyberturvallisuuden asiantuntijatalo, joka palvelee yrityksiä ja muita organisaatioita vahvistamalla ja kehittämällä valmiuksia suojata ja puolustaa niiden merkittävimpiä toimintoja.

Missiomme: kyberturvallisuudesta bisnesmahdollisuus

Cyberwatch Finland palvelee yrityksiä ja muita organisaatioita vahvistamalla ja kehittämällä niiden kyberturvallisuuskulttuuria.

Tiukentuva sääntely parantaa kaikkien kyberturvallisuutta, mutta vähimmäisvaatimusten noudattaminen ei riitä yhä kiristyvässä kilpailussa. Korkeatasoinen kyberturvallisuuskulttuuri on kilpailuetu ja luo uusia liiketoimintamahdollisuuksia.

Laaja-alainen osaaminen, kokemus ja näiden uniikki yhdistelmä on vahvuutemme

Asiantuntijatiimimme koostuu strategisen kyberturvallisuuden monipuolisesta osaamisesta, jota täydentää laaja-alainen kokemus johtamisesta, kokonaisturvallisuudesta ja toiminnasta kansainvälisessä yritysympäristössä.

Asiantuntijoillamme on kyky tulkita ja esittää monimutkaisia kybermaailman ilmiöitä ja kehityskulkuja helposti ymmärrettävässä muodossa. Käytämme työssämme hyväksi kehittyneitä teknisiä alustoja ja analytiikkatyökaluja.

”Autamme asiakasta pysymään ajan tasalla ja kehittämään kyberturvallisuuskulttuuria johdonmukaisesti. Samalla rakennamme yhdessä kestävämpää ja turvallisempaa maailmaa”

Aapo Cederberg, Cyberwatch Finlandin toimitusjohtaja ja perustaja

PALVELUMME

Johdon neuvontapalvelut

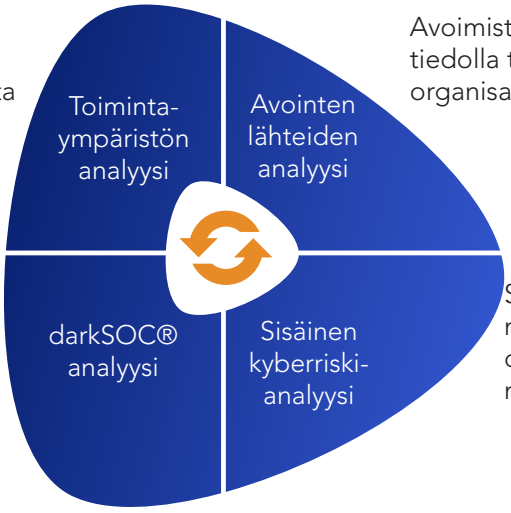
Olemme kokenut ja luotettu johdon neuvonantaja ja asiantuntija. Tuemme sinua kokonaisturvallisuuden, kyberturvallisuuden, sisäisen turvallisuuden asiakokonaisuuksissa ja kumppaniriskien hallinnassa. Työskentelymetodeinamme ovat muun muassa teema-alustukset, muistiot, työpajat ja skenaariotyöskentely.

Toimintaympäristön tilannekuva

Kokonaisvaltainen kybertilannekuva muodostuu Cyberwatch Finlandin kehittämän modulaarisen palvelun avulla, johon tarvittavaa dataa kerätään lukuisin eri menetelmin.

Toimintaympäristön analyysilla muodostetaan eri näkökulmista kuva organisaatioon vaikuttavista tapahtumista, ilmiöistä ja trendeistä.

Pimeän ja syvän verkon dataa kerätään ympäri maailmaa sijaitsevilla palvelimilla taukoamatta 9 Gb sekunnissa.



Avoimista lähteistä kerätyllä tiedolla täydennetään organisaatiosta saatua kuvaa.

Sisäisen kyberriskianalyysin avulla muodostetaan kokonaiskuva organisaation sisäpiiriuhkista ja muista riskitekijöistä.

PALVELUMME

Tilannekatsaukset

Cyberwatchin analyysitiimi seuraa jatkuvasti kyberturvallisuuden toimintaympäristöä keräämällä ja analysoimalla tietoa kybermaailman tapahtumista, ilmiöistä ja muutoksista. Tilannekuvaa tuotetaan säännöllisillä tilannekatsauksilla.

Viikkokatsaus

Viikkokatsauksessa esitellään kybertoimintaympäristön ajankohtaisia tapahtumia ja on luonteeltaan toteava.
Keskeistä viikkokatsauksessa on ilmiöiden ja trendien tunnistaminen ja niiden asettaminen asianmukaiseen viitekehykseen.
Viikkokatsaukset toimivat pohjana kuukausikatsauksille sekä vuosiennusteille.
Viikkokatsauksen avulla saat ajantasaista kuvaa merkittävistä kybermaailman tapahutumista päätöksenteon tueksi.
Viikkokatsaus ilmestyy 52 kertaa vuodessa suomeksi ja englanniksi.

Kuukausikatsaus

Kuukausikatsauksessa analysoidaan viikkokatsauksissa seurattuja tapahtumia, trendejä ja niiden keskinäisvaikutuksia.
Kuukausikatsaus kuvaa ilmiöiden kehittymistä erityisesti hybridivaikuttamisen eri näkökulmista.
Kuukausikatsauksen avulla saat syvempää näkemystä siitä, kuinka kybermaailman tapahtumat vaikuttavat yhteiskuntaan ja toimintaympäristöösi.
Kuukausikatsaus ilmestyy 12 kertaa vuodessa suomeksi ja englanniksi.

Cyberwatch Magazine

Cyberwatch magazine on digitaalinen ja painettu aikakauslehtijulkaisumme, jossa omat ja verkostomme huippuasiantuntijat kirjoittavat kybermaailman ajankohtaisista tapahtumista, teknologian ja lainsäädännön kehityksestä ja näiden vaikutuksesta yhteiskuntaan, organisaatioihin ja yksittäisiin ihmisiin.

Special reports

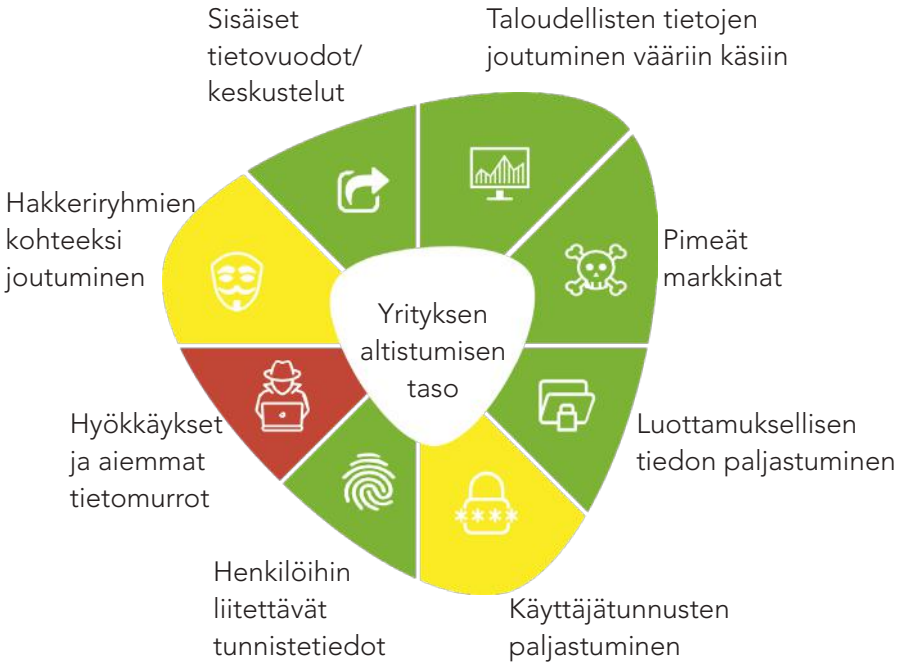
Tuotamme määrittelemästäsi teemasta, esimerkiksi tietystä toimialasta tai kohdemarkkinasta raportteja ja katsauksia: nykytilan arviointeja, uhka-arvioita, toimintaympäristöanalyyseja ja ennusteita

PALVELUMME

darkSOC® –pimeän ja syvän verkon analyysi

DarkSOC® -analyysin avulla selvitämme organisaatiosi profiilin ja altistumisen tason pimeässä ja syvässä verkossa. Dataa kerätään ympäri maailmaa sijaitsevilla palvelimilla taukoamatta 9 Gb sekunnissa. Analyysi paljastaa organisaatiosi kyberturvallisuuden puutteita, vuotaneita tietoja ja muita mahdollisia ongelmakohtia. Analyysin avulla saat näkemyksen siitä, miltä organisaatio näyttää kyberrikollisen silmin katsottuna.

Luokittelemme kyberaltistumisen vaikutukset kahdeksaan kategoriaan. Laadimme analyysista kirjallisen raportin, jossa tuomme esille keskeiset havainnot johdon päätöksenteon tueksi. Raportti sisältää myös havaintojen yksityiskohtaisemman esittelyn. Annamme lisäksi suosituksia välittömistä korjaavista toimista ja strategisen tason kehityskohteista.



MITÄ HYÖTYJÄ darkSOC® -PALVELU TARJOAA

- Lisää kybertiedustelu-kykyä
- Ennakoi kyber-maailman kehityskulkuja
- Täydentää yrityksen kyber-maturiteettia
- Toimii forensic-tutkinnan apuvälineenä
- Tukee organisaation strategista päätöksentekoa
- Täydentää strategista kybertilanne-kuvaa
- Löytää haavoittu-vuuksia ja heikkouksia
- Fasilitoi kyberstrategia-prosessia

PALVELUMME

Analyysit

Pintaverkon analyysi

Muodostamme ulkopuolisen näkemyksen kyberturvallisuuden tasostasi pintaverkossa ja vertaamme asemaasi muihin saman toimialan organisaatioihin. Analyysimme pohjana on globaalin yhteistyökumppanimme SecurityScorecardin alusta, jonka data perustuu luotettuun, läpinäkyvään luokitusmenetelmään ja miljoonista organisaatioista kerättyihin tietoihin. Analyysimme perusteella annamme suosituksia korjaavista toimenpiteistä ja rakennamme reittikartan niiden käytännön toteuttamiselle organisaatiossasi.

Powered by Security Scorecard

Avoimien lähteiden analyysi

Tuotamme avoimiin lähteisiin perustuvia analyyseja valitsemistanne aiheista. Käytössämme on edistyneitä digitaalisia työkaluja, joiden avulla haemme tietoa julkisista maksuttomista ja maksullisista lähteistä sekä eri medioista ja sosiaalisen median alustoilta. Jalostamme tiedon analyysin tavoitteiden kannalta merkitykselliseen muotoon.

Sisäinen kyberriskianalyysi

Sisäisen kyberriskianalyysin avulla muodostat kokonaiskuvan organisaatiosi kyberturvallisuuteen liittyvistä sisäpiiriuhkista ja muista riskitekijöistä.

Analysoimme organisaatiosi kyberturvallisuuteen liittyvän ohjeistuksen ja muun dokumentaation ajantasaisuuden ja kattavuuden. Lisäksi haastattelemme johtoa ja muuta avainhenkilöstöä.

Analyysin tuloksena saat kuvan organisaatiosi toiminnan ja sitä ohjaavien sisäisten ohjeiden ja ulkoisen sääntelyn välisestä tasapainosta sekä tiekartan toiminnan kehittämiseksi.

PALVELUMME

Analyysit

NIS2 Konsultaatio ja koulutus

NIS2 kyberturvallisuus direktiivin tavoitteena on parantaa kyberturvallisuuden perustasoa EU:n alueella ja varmistaa kriittisten toimijoiden toiminnan jatkuvuus.
Direktiivi tuli voimaan 17.1.2023, jäsenmaissa aikaa laittaa asiat kuntoon 17.10.2024 mennessä.

NIS2 kyberturvallisuus direktiivi koskee seuraavia toimialoja:

NIS2 kyberturvallisuus direktiivin vähimmäisvaatimukset ovat:

1. Riskianalyysia ja tietojärjestelmien turvallisuutta koskevat politiikat
2. Poikkeamien käsittely
3. Toiminnan jatkuvuuden hallinta, kuten varmuuskopiointi ja palautus sekä kriisinhallinta
4. Toimitusketjun turvallisuus
   - Riskiperusteisuus
   - Datan kanssa tekemisissä olevat
5. Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja paljastaminen
6. Periaatteet ja menettelyt kyberturvallisuusriskien hallintatoimenpiteiden tehokkuuden arvioimiseksi
7. Kyberhygienian peruskäytännöt ja kyberturvallisuuskoulutus
8. Salauksen ja kryptografian käyttöä koskevat käytännöt ja menettelyt
9. Henkilöresurssien turvallisuus, kulunvalvontakäytännöt ja omaisuudenhallinta
10. Vahvennetun todennuksen tai jatkuvan todennusratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä turvattujen hätäviestintäjärjestelmien käyttö yksikön sisällä.

Oman organisaation nykytilan vastaavuus vähimmäisvaatimuksiin kannattaa aloittaa hyvissä ajoin. Cyberwatchin NIS2 puuteanalyysi on vähimmäisvaatimuksia riskiperusteisesti lähestyvä malli, jossa viitekehyksenä käytetään paitsi direktiiviä, myös ISO 27001 standardia ja siihen liittyviä hallintakeinoja. Analyysin avulla organisaatio voi suunnata kehittämistoimet juuri oikeisiin kohteisiin.

PALVELUMME

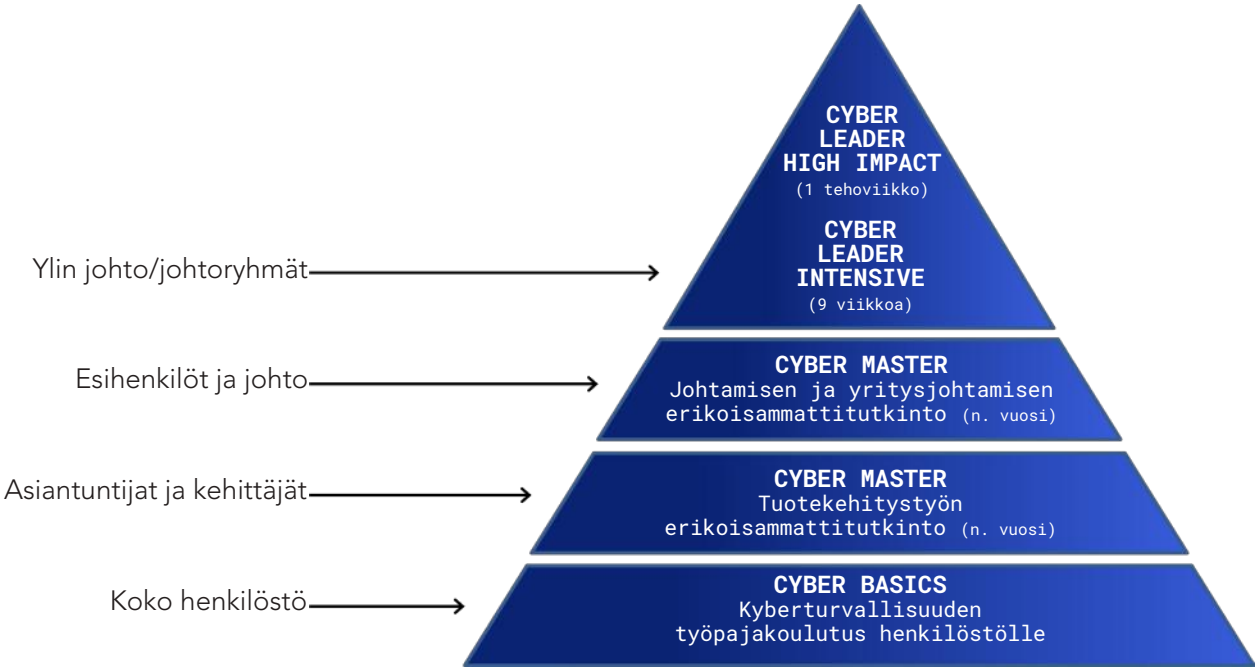
Koulutus ja osaamisen kehittäminen

Tuotamme yhdessä Management Institute of Finlandin (MIF) kanssa Cyber Master erikoisammattitutkintokoulutusta.

Tällä hetkellä ohjelmissa voi suorittaa Johtamisen ja yritysjohtamisen Cyber Master erikoisammattitutkinnon sekä tuotekehityksen Cyber Master erikoisammattitutkinnon.

Toteutamme organisaatiollesi myös räätälöityjä koulutuksia, joiden avulla vahvistat kyberturvallisuuden osaamista ja valmistaudut kohtaamaan digitaalisen toimintaympäristön haasteita.

Kaikki koulutustarjontamme koostuu moduuleista, joista opiskelija tai organisaatio voi valita tilanteeseen tai toimintaan soveltuvat osat.



INTOHIMONA KYBERTURVALLISEMPI MAAILMA

Ota yhteyttä

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi

CYBER SECURITY NORDIC

Two stages packed with cybersecurity insights from leading companies and global experts

AMONG THE HEADLINE SPEAKERS ARE:

William H Dutton
Martin Fellow at Oxford University's Global Cyber Security Capacity Centre

Cybersecurity Capacity Building: The Whats, The Whys and The Hows
Tuesday 29 Oct | 11:45–12:15

Prof. William H. Dutton, Martin Fellow at Oxford University's Global Cyber Security Capacity Centre is among the most interesting Keynote speakers. He was the founding director of the OII, the first Professor of Internet Studies at Oxford University, and an Emeritus Professor at the University of Southern California. His most recent book is The Fifth Estate: The Power Shift of the Digital Age (OUP 2023).

Max Schrems
Lawyer, author, privacy activist
NOYB – European Center for Digital Rights

Privacy in a global world
Wednesday 30 Oct | 13:15–13:45

Max Schrems, a renowned privacy advocate and representative of NOYB – European Center for Digital Rights, will be among the notable speakers also in CSN 24. Schrems gained international recognition for his groundbreaking campaigns against Facebook (Meta), exposing privacy violations, including violations of European privacy laws. Noyb.eu has also recently filed a complaint against OpenAI with the Austrian DPA and is going to challenge the third attempt of EU-US data transfers agreement.

JM Monteith
LM Fellow | Cyber, Lockheed Martin

The Evolving Threat to Critical Technologies
Wednesday 30 Oct | 11:45–12:15

Mr. Monteith representing the US Lockheed Martin has 20+ years Cyber Security Architecture and Engineering experience in the Aerospace and Defence industry. Mr. Monteith has led enterprise initiatives in collaboration with, or in support of, Foreign Military Sales (FMS) customers, US and foreign government customers, partners, and suppliers, to develop, deploy and sustain IT and cyber solutions incorporating the full stack of information technology domains.

Hacker's Corner – a new addition for 2024

A new feature at Cyber Security Nordic 2024 is the Hacker's Corner, where hands-on cybersecurity professionals are invited to test their skills in real-world scenarios and compete against each other. Participants will collaborate with leading cybersecurity companies to solve complex security challenges, diving into the mind of a hacker and tackling various puzzles.

The participating companies offering the challenges are:
Trend Micro – Focus on Red Teaming CTF | **Insta** – Intruders-demo | **WithSecure** – "Macbooks can't get viruses" | **Nixu** – Save Lucy from the dark! | **Vectra AI** | **Truesec**

MESSUKESKUS
The real social media

FOR A BETTER DIGITAL FUTURE

Technology and digitalisation are changing people's behaviour, business practices, and market dynamics. Cyber Security Nordic will explore cybersecurity from the perspectives of both businesses and public administration. The speeches will cover topics such as the impact of digitalisation on democracy and technology regulations, the increasing diversity of cyber-attacks, and approaches to risk management for critical functions of companies and societies.

Explore more and register free-of-charge:
cybersecuritynordic.com

CYBER SECURITY NORDIC

29–30 October 2024
Helsinki Expo and Convention Centre