Strategisen kyberturvallisuuden erikoisjulkaisu

Cyberwatch Finland

MAGAZINE 1/2024

HYBRIDISODANKÄYNTI ON JATKUVAA INFORMAATIOVAIKUTTAMISTA

KRIISIVIESTINTÄ VAHVISTAA RESILIENSSIÄ

DISINFORMAATION JA ULKOMAISEN VAIKUTTAMISEN TORJUNTA TEKOÄLYN AIKANA

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

SISÄLLYS

1/2024

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 Turunen
elina@cyberwatchfinland.fi

ULKOASU JA TAITTO
Elina Turunen
elina@cyberwatchfinland.fi

KUVITUS
Gencraft
Pixabay
Shutterstock

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

PAINO
Scanseri Oy, Helsinki

HYBRIDISODANKÄYNTI ON JATKUVAA INFORMAATIOVAIKUTTAMISTA

// Aapo Cederberg

Elämme epävakaassa maailmassa. Kulutussota Ukrainassa, Gazan konflikti, terroristien iskut kauppalaivoihin sekä alueelliset kriisit Afrikassa uutisoidaan meille kaikkia kanavia pitkin jatkuvana informaatiotulvana. Olemme siten jatkuvan informaatiovaikuttamisen kohteena, halusimme tai emme, ja turvallisuuden tunteemme on horjunut. Kyberhyökkäykset ovat usein vaikeasti hahmotettavissa, ja niiden päämääristä, tekijöistä tai toteuttamistavasta ei yleensä ole täyttä varmuutta. Selkeimmin hyökkäysten seurannaisvaikutukset näkyvät esimerkiksi yhteiskunnan elintärkeiden toimintojen häiriöinä. Epävarmuus aiheuttaa meissä ihmisissä pelkoa ja levottomuutta sekä tyytymättömyyttä modernin yhteiskunnan palveluiden luotettavuuteen. Nämä kanavoituvat usein kritiikkinä poliittisia päätöksentekijöitä ja palveluita tuottavia yrityksiä kohtaan. Vaikutukset saattavat olla hyvinkin pitkäkestoisia ja salakavalia.

Usein informaatiosodankäynti ja -vaikuttaminen mielletään väärän tiedon levittämiseksi, valeuutisiksi, tiedon ja datan manipuloimiseksi. Toki ne ovat sitäkin. Silloin tavoitteena on usein lyhyemmän tähtäyksen päämäärät ja vaikuttaminen esimerkiksi johonkin tiettyyn poliittiseen prosessiin. Tarinat eli narratiivit vaikuttavat usein kovin utopistisilta ja epäuskottavilta, mutta niiden tarkoitus voikin olla vaikuttaa johonkin kohderyhmään tai vaikkapa autoritäärisen valtion sisäpolitiikkaan. Tekoäly tuottaa koko ajan uusia mahdollisuuksia esimerkiksi tiedon manipulointiin, syvävääreennyksiin ja erilaisiin huijauksiin. Dis- ja misinformaatiolta länsimainen valveutunut media ja kansalaiset ovat oppineet suhteellisen hyvin suojautumaan. Vähemmälle huomiolle on jäänyt erilaisten hybridioperaatioiden informaatiovaikutusten analysointi ja niiltä suojautuminen. Se on pitkäkestoista ja kätkeytyy epämääräisyyden kuten ns. sodan sumun varjoon.

Venäjä sanoo käyvänsä sivilisaatioiden välistä kampailua länsimaita vastaan, josta hyökkäyssota Ukrainassa on vain yksi rintama. Venäjän yleisesikunta-akatemian määrittelyn mukaan sota jakautuu perinteiseen sodankäyntiin ja hybridisodankäyntiin. Kummassakin käytetään sekä fyysisiä keinoja eli sotilaallista voimaa että epäsymmetrisiä keinoja, kuten kyberhyökkäyksiä, informaatio-operaatioita, poliittista painostusta, sabotaasitoimintaa, pakolaisvirtoja, talouspakotteita sekä energia-asetta. Suomessa on selvästi huomattu, että olemme jatkuvan hybridisodankäynnin kohteena, jonka tavoitteena on luoda epävarmuutta, pelkoa ja eripuraa kansalaisten keskuudessa ja siten epäsuorasti vaikuttaa poliittiseen päätöksentekoon. Tässäkin sodankäynnin muodossa korostuu yllätyksellisyys, aloitteellisuus ja erilaiset harhauttamisen keinot. Kaikki nämä tehostavat haluttuja informaatiovaikutuksia, joiden onnistuminen edellyttää ihmismielen ja perustarpeiden sekä haavoittuvuuksien hyväksi käyttämistä. Vaikutukset voivat olla pitkäkestoisia ja ennalta-arvaamattomia. Hybridisodankäynnin ”strateginen ase” onkin pitkäkestoinen informaatiovaikuttaminen, jota vastaan meidän on opittava paremmin suojautumaan. Maalina on koko yhteiskunta ja kansalaisten henkinen selkäranka.

Natossa on ryhdytty voimakkaasti panostamaan kognitiiviseen sodankäyntiin ja puolustukseen. Ensimmäiseksi tulee mieleen, yritetäänkö pyörää keksiä uudestaan, vai onko tässä todella uusi sodankäynnin muoto. Naton mukaan se on kehittämässä uudenlaisia sodankäynnin muotoja voidakseen käydä “taistelua aivoista”, niin kuin sotilasliitto asian ilmaisee. Tässä konseptissa kokeillaan uudenlaisia hybridisodankäynnin muotoja tunnistettuja vihollisia vastaan, käyttäen hyväksi mm. taloussodan, kybersodan, informaatiosodan ja psykologisen sodankäynnin menetelmiä. Uusi metodi on “aivotieteiden asekäyttöön ottamista”, ja siinä “hakkeroidaan henkilö” käyttämällä hyväksi “ihmisaivojen heikkouksia” sofistikoituneemman “yhteiskunnallisen manipuloinnin” aikaansaamiseksi. Tavoitteena näyttäisi olevan, ei pelkästään suojautuminen, vaan myös aktiivisten keinojen kehittäminen ja käyttäminen.

Natossa ollaan siis ajan hermolla ja tarve ”hybridipuolustuksen” kehittämiselle on tunnistettu. Suomi on liittokunnan uutena ja aktiivisena jäsenenä mukana tälläkin osa-alueella. Hyvän pohjan meille antaa suomalainen kokonaisturvallisuuden malli ja ennen kaikkea osaamisemme henkisen kriisinsietokyvyn kehittämisessä. Näistä elementeistä syntyy toivottavasti riittävä resilienssi Venäjän pitkäkestoista informaatio-operaatiota vastaan. ■

AAPO CEDERBERG

- Toimitusjohtaja ja perustaja
- **Cyberwatch Finland**

DISINFORMAATION JA ULKOMAISEN VIHAMIELISEN VAIKUTTAMISEN TORJUNTA TEKOÄLYN AIKANA

// Pasi Eronen Watt

CYBERWATCH FINLAND

Olemme viime vuosina saaneet todistaa generatiivisen tekoälyn edistysaskeleita ja valtavaa harppausta eteenpäin. Tekoäly on siirtynyt kulissien takaisista tehtävistä, kuten sisällön suosittelusta, lähes itsenäiseen tekstin, äänen, videon ja kuvien sisällöntuotantoon. Yhä tehokkaampien tekoälytyökalujen leviäminen työpaikoille ja eri järjestelmiin on väistämätöntä. Innovaatiokeskittymät, kuten Piilaakso, keksivät tekoälylle uusia jatkuvasti käyttötarkoituksia.

Open AI:n Chat GPT, DALL-E ja tuleva Sora ovat näkyvimmät suurelle yleisölle saatavilla olevista työkaluista, mutta tällä alueella on saatavilla myös suuri joukko sekä suljetun että avoimen lähdekoodin työkaluja. Joissakin näistä työkaluista on vähemmän ennalta asetettuja rajoituksia niiden epäeettiselle käytölle.

Tekoälyn kehitys on luonteeltaan nopeatempoista, mikä tekee haastavaksi tutkijoille, päätöksentekijöille ja yleisemmin yhteiskunnille pysymisen sen viimeisimpien edistysaskeleiden tasalla. Se myös vaikeuttaa tehokkaiden vastatoimien suunnittelua ja toteuttamista tekoälyn tuottamaa manipulointia ja disinformaatiota vastaan. Tämä viive voi jättää yhteiskunnat alttiiksi tekoälyn tuottamalle disinformaatiolle.

Myös vihamieliset toimijat ympäri maailmaa, kuten Venäjä ja Kiina, sekä rikolliset seuraavat kehitystä. Ne hankkivat, tutkivat, kehittävät ja ottavat käyttöön kehittyneitä tekoälyyn perustuvia teknologioita kokeillakseen niitä tiedon manipulointi ja disinformaatiokampanjoissaan.

MIKSI ASIA ON TÄRKEÄ?

Tekoälyn käyttö aseena mahdollistaa tiedon manipuloinnin ja disinformaatiokampanjat. Niiden seuraukset voivat horjuttaa monin tavoin yhteiskuntia ja jaettua turvallisuuden tunnetta:

- Ensisijaisina kohteina voidaan pitää haavoittuvassa asemassa olevia ja syrjäytyneitä väestöryhmiä, kuten maahanmuuttajia ja ihmisiä, joilla on vaikeuksia osallistua yhteiskuntaan ja sen toimintaan ja joilla on heikommat mahdollisuudet käyttää luotettavia tietolähteitä. Heidän luottamuksensa viranomaisiin ja instituutioihin voi järjestelmällisesti murentua.

- Demokratioiden poliittisia prosesseja ja hallintoja voidaan heikentää yleisen mielipiteen järjestelmällisellä manipuloinnilla. Tästä tulee vielä suurempi ongelma, kun teknologisen kehityksen myötä totuus tai todellisuus muuttuu erottamattomammaksi tekoälyn luomista valheista.
- Erittäin realistiset syväväärennökset (deep fakes), kuten valokuvat ja videot tai ääninauhat, voivat vaikuttaa psykologisesti merkittäviin henkilöihin, kuten poliitikkoihin, taiteilijoihin, tai ryhmiin. Heidän maineensa voi kärsiä ja yksityisyyden tunteensa horjua tekoälyn tuottamien väärennösten myötä.
- Sosiaalisen median kaikukammiot ja algoritmien optimoimat sosiaalisen median kuplat vahvistavat dramaattisesti disinformaation mahdollisia vaikutuksia, koska huolellisesti räätälöity sekä kohdennettu sisältö auttaa luomaan polarisoituneita yhteisöjä, jotka eivät jaa keskenään edes perusfaktoja tai totuutta.
- Laajamittaisia tekoälybottien automatisoituja ja autonomisia disinformaatiokampanjoita on haastavaa tunnistaa ja torjua. Erityisesti, jos tekoälytyökaluja käytetään tavalla, joka sallii viestien sisällön vaihtelun kontekstin mukaan sen sijaan, että toistettaisiin yhtä ja samaa viestiä kaikilla väärennetyillä tileillä. Tämä antaa vastustajillemme mahdollisuuden luoda ja levittää nopeasti useita "vastakertomuksia", joita voidaan käyttää hämmentämään yleisöä, erityisesti nopeasti kehittyvässä tilanteessa.
- Riittävällä tilannekohtaisella ymmärryksellä ja tekoälyn hienosäädöllä kohdeyleisöjen mukaan, tekoälyn tuottama sisältö on mahdollista suunnitella hyödyntämään olemassa olevia ja tunnistettuja ihmisen kognitiivisia vinoumia ja emotionaalisia tekijöitä. Tämä voi toimia keinona manipuloida yksilöllistä käyttäytymistä ja käsityksiä myös reaalimaailman puolella.

> **Tekoäly on siirtynyt kulissien takaisista tehtävistä, kuten sisällön arvostelusta ja suosittelusta, lähes itsenäiseen tekstin, äänen, videon ja kuvien sisällöntuotantoon.**

ONKO ONGELMAAN RATKAISUJA?

Tekoälyä hyödyntävän manipulointi- ja disinformaatiokampanjoiden torjumiseksi ei ole olemassa yksinkertaisia ihmeratkaisuja. Siitä huolimatta on olemassa joitain tapoja pyrkiä hallitsemaan käsillä olevaa ongelmaa ja lieventämään sen vaikutuksia.

Lieventävät ratkaisut edellyttävät maailmanlaajuista yhteistyötä, julkista koulutusta, medialukutaitoa, etiikkaa ja avoimuutta tekoälyn kehittämisessä, vastuullisuutta teknologia-alustojen omistajilta sekä jatkuvaa tutkimusta ja sopeutumista uusien uhkien ilmaantuessa:

- **Yleinen tietoisuus:** Yleisen tietoisuuden lisääminen tekoälyn tuottaman disinformaation mahdollisuuksista on ratkaisevan tärkeää sen vaikutusten lieventämiseksi. Disinformaation leviämistä voidaan torjua kouluttamalla ihmisiä tunnistamaan tekoälyn tuottama sisältö ja kannustamalla terveeseen skeptisyyteen vahvistamatonta tietoa kohtaan.
- **Koulutus ja medialukutaito:** Laajat julkiset valistuskampanjat ja medialukutaidon sisällyttäminen koulujen opetussuunnitelmiin kehittävät kansalaisten ja keskeisten ryhmien, kuten toimittajien ja opettajien, taitoja tunnistaa tekoälyn luomaa disinformaatiota ja arvioida lähteitä kriittisesti. Tämä ruohonjuuritason lähestymistapa parantaa yhteiskunnan resilienssiä, mutta se on sangen pitkän aikavälin lähestymistapa.

Artikkelin laadinnassa on hyödynnetty Open AI:n ChatGPT-4 ja Anthropicin Claude -palveluja.

- **Eettinen vastuu:** Generatiivisen tekoälyn kaltaisilla teknologioilla on merkittävä potentiaali sekä hyvään että haitalliseksi katsottavaan toimintaan. Näitä järjestelmiä kehittävien tutkijoiden ja innovaattoreiden on noudatettava eettisiä periaatteita ja otettava vastuuta myös luomiensa työkalujen mahdollisista haitallisista seurauksista. Kehitystyö tulee mahdollisuuksien mukaan sovittaa yhteen kehittyvän kansallisen ja kansainvälisen lainsäädännön ja normiston kanssa. Tämä siitä huolimatta, että tuskin voimme pakottaa vastustajamme noudattamaan samoja eettisiä sääntöjä kuin me.
- **Maailmanlaajuinen yhteistyö:** Tiedon manipulointi ja disinformaatio ylittävät kansalliset rajat. Kansainväliset normit, tiedon ja datan jakamista koskevat aloitteet luotettujen kumppaneiden kesken sekä rahoitus vastatoimien kehittämiseen voivat mahdollistaa yhtenäisen rintaman tekoälyn vahvistamaa ulkomaista vihamielistä vaikuttamista vastaan. Koordinoidut diplomaattiset, taloudelliset ja oikeudelliset toimet disinformaation valtiollisia tukijoita ja niiden ylläpitäjiä vastaan voivat myös toimia pelotteina.
- **Teknologia-alustojen vahvempi sääntely:** Sosiaalinen media ja sivustot on pakotettava lainsäädännöllä ottamaan aktiivisempi asenne sisällön moderointiin, disinformaatiobottien poistamiseen, valesisältöä tukevan algoritmin minimoimiseen ja avoimuuteen käytännöistään, mukaan lukien algoritmit. Sääntelyssä on kuitenkin otettava huomioon maailmanlaajuisen kilpailun epätasapaino, jossa oikeudellisesta näkökulmasta sallivammissa ympäristöissä

kehitetyt alustat voivat saada epäoikeudenmukaista kilpailuetua säännellympiin ympäristöihin nähden.

- **Jatkuva tutkimus- ja kehitystoiminta:** "Tekoälyn kilpavarustelu" erilaisia vastustajia vastaan on sekä väistämätöntä että välttämätöntä ja edellyttää jatkuvia teknologisia investointeja tekoälyn luoman mediasisällön merkitsemiseksi, disinformaatioverkostojen tunnistamiseksi ja muiden vastatoimien kehittämiseksi. Toimintaympäristön kehittymisen tarkka seuranta on ratkaisevan tärkeää, erityisesti vihamielisten valtioiden osalta.
- **Resilientit tietoekosysteemit:** Reaktiivisten vastatoimien lisäksi tarvitaan pyrkimyksiä rakentaa kansallisia ja ylikansallisia mediaekosysteemejä, joissa on tunnistettuja luotettavia tietokuraattoreita, erilaisia näkökulmia ja algoritmit ovat läpinäkyviä. Nämä voivat tehdä yhteiskunnista vastustuskykyisempiä vihamieliselle manipuloinnille.
- **Muutoksen omaksuminen:** Sen sijaan, että väärinkäytöksille alttiita tekoälyteknologioita vastustettaisiin tai sokeasti kiellettäisiin, niiden ennakoiva omaksuminen ja integrointi eri aloilla voi lisätä ymmärrystä ja edistää suojatoimiin sekä mahdollisiin vastatoimiin liittyvää innovointia. Esimerkiksi hyödyntämällä generatiivista tekoälyä luokkahuoneissa, yrityksissä ja valtion virastoissa, voidaan kehittää parhaita käytäntöjä, paljastaa ratkaisuja vaativia riskejä ja luoda joukko kansalaisia, jotka sietävät paremmin disinformaatiota omakohtaisen kokemuksen ansiosta. Joustava, tulevaisuuteen suuntautuva ajattelutapa tunnistaa mahdolliset hyödyt vaarojen rinnalla.

Tulevaisuudessa tekoälyllä on valtava potentiaali parantaa ihmisten elämää sen eri osa-alueilla niin kodeissa kuin työpaikoillakin. Edistyksessä on kuitenkin jatkuvasti tasapainoiltava ja tekoälyn käytännön riskit on tunnustettava rehellisesti. Edellä esitettyjen haitallisten vaikutusten lieventämiseen tarkoitettujen ratkaisujen huolellisella soveltamisella yhteiskunnat voivat hyödyntää tekoälyn voimaa ja samalla ylläpitää informaatioympäristöä, joka on myös kestää siihen kohdistuvat vaikuttamisyritykset ja muut iskut.

Generatiivisen tekoälyn rajoittamattoman kehityksen aiheuttamia vaaroja ei voida sivuuttaa, sillä kilpailijat pyrkivät eittämättä hyödyntämään myös sen negatiivisia käyttötarkoituksia. Emme voi pysäyttää tai kääntää kehitystä, ja samalla antaa vastustajiemme kiriä edellemme. Siksi olisi tärkeä varmistaa, että pysymme käynnissä olevassa kamppailussa kanssakilpailijoiden edellä, jotta voimme suojella yhteiskuntiamme niiltä, jotka tahtovat meille pahaa.■

PASI ERONEN WATT

Pasi Eronen Watt on kansainvälisiin turvallisuuskysymyksiin keskittynyt analyytikko ja kirjoittaja, joka on erikoistunut informaatiovaikuttamiseen ja kyberturvallisuuteen. Hänellä on laaja kokemus työskentelystä valtionhallinnossa, mukaan lukien kansainväliset tehtävät.

MITÄ OVAT MISINFORMAATIO, DISINFORMAATIO JA FIMI?

Misinformaatiolla tarkoitetaan väärää tai virheellistä tietoa, jota levitetään tahattomasti pelkän tietämättömyyden tai rehellisten virheiden vuoksi. **Disinformaatio** taas on väärää tietoa, jota levitetään tietoisesti harhaanjohtamisen tai vahingon aiheuttamistarkoituksessa.

Foreign information manipulation and interference (FIMI), eli ulkomainen tiedon manipulointi ja häirintä, on sekä EU:n että Naton omaksuma käsite. Se kattaa vihamielisten valtiollisten tai valtiosta riippumattomien toimijoiden toteuttamat koordinoidut disinformaatiokampanjat, joilla horjutetaan yhteiskuntia, heikennetään luottamusta instituutioihin ja puututaan poliittisiin prosesseihin.

FIMIn kaltaisen käsitteen tekee erityisen tärkeäksi se, että manipuloinnin ei tarvitse perustua valheeseen, vaan se voi olla myös poliittisten tai muiden vilpittömästi ilmaistujen näkemysten keinotekoista vahvistamista, jotka palvelevat ulkomaisen vastustajan agendaa ja poliittisia tavoitteita.

VENÄJÄN JA UKRAINAN KONFLIKTI HYBRIDISODANKÄYNNIN NÄKÖKULMASTA – KAKSI VUOTTA SOTAA

// Josef Schroefl ja Soenke Marahrens

* Tämä artikkeli perustuu HybridCoE:n kirjoittajien sisäisiin ja ulkoisiin julkaisuihin

HYBRIDIELEMENTTI VENÄJÄN HYÖKKÄYKSESSÄ UKRAINAAN

Länsimaiset sotilasstrategit ovat kehittäneet lyhenteen VUCA (volatility, uncertainty, complexity ja ambiguity) kuvaamaan tulevaisuuden toimintaympäristön ominaisuuksia - volatiliteettia, epävarmuutta, monimutkaisuutta ja epäselvyyttä. Pessimistisemmin voidaan käyttää myös BANIa (brittle, anxious, nonlinear ja incomprehensible), joka tarkoittaa haurasta, ahdistunutta, epälineaarista ja käsittämätöntä. Voidaankin sanoa, että venäläiset ovat olleet erittäin dynaamisia ja tarkkoja luodessaan, joko tarkoituksella tai tahattomasti, VUCA- tai BANI-olosuhteet länsimaille.

Hybridisota on ilmiö, joka elää jatkuvasti. Myös hybridisodankäynti (joka perustuu erityisesti sotilaallisin keinoin toteutettuihin hybridiuhkiin) on ilmiölle vielä välitermi. Hegeliläisessä mielessä "hybridisota" voidaan nähdä sodan antiteesinä maailmassa, jossa sota on sijoitettu kansainväliseen humanitaariseen oikeuteen ja lopulta kielletty pakottamalla kaikki kansakunnat allekirjoittamaan YK:n peruskirjan. Mutta synteesi puuttuu edelleen.

Hybridiosaamiskeskuksen mukaan hybridiuhkatoiminnalle (joka sisältää uhkat ja sodankäynnin) voidaan erottaa neljä ominaisuutta:

1. Se ei ole yksittäinen tapahtuma.
2. Se tarvitsee pahaa aikovan tarkoituksen/toimijan.
3. Sitä toteuttavat autoritaariset järjestelmät, jotka haastavat demokraattisia sääntöpohjaisia yhteiskuntia.
4. Harmaan vyöhykkeen luo puolustaja, ei hyökkääjä, jälkimmäinen vain käyttää hyväkseen puolustajan haluttomuutta asettaa punaiset viivansa.

Antagonisti käyttää hyväkseen joko kohdevaltion haluttomuutta puolustaa sääntöjä tai luotujen lakien ja sääntöjen monimutkaisuutta, mikä antaa pahantahtoiselle toimijalle mahdollisuuden joko käyttää näitä sääntöjä väärin tai luoda ongelmia sääntöjen sovellukseen.

VENÄJÄN SOTATOIMET UKRAINASSA HYBRIDISODAN LINSSIEN LÄPI KATSOTTUNA:

Venäjän hybridiuhkakampanja Ukrainaa vastaan ennen 24. helmikuuta 2022 oli strateginen mestariteos. Yhdysvallat, Nato ja EU eivät olleet varmoja siitä, mitä todella tapahtui. Hybridiuhkatoimet herättivät pelkoa Baltian maissa, Ruotsissa ja Suomessa. Hybridioperointi oli erittäin ketterää, etsien jatkuvasti lännen heikkoja kohtia ja sekaantuen niihin lähes välittömästi oikeudellisin, informaatio-, disinformaatio- ja diplomaattisin keinoin, joihin yhdistyi melko pitkä sotilaallinen voimannäyttö Ukrainan ympärillä, mikä lisäsi yleistä epävarmuutta.

Sotilaallisten tapahtumien vähemmän onnistuneeseen etenemiseen 24. helmikuuta 2022 jälkeen, jolloin Venäjän joukot eivät kyenneet hyödyntämään oletettua strategista ketteryyttään. Tämä saattoi aiheuttaa jonkinlaisen strateginen romahduksen Putinin sisäpiirissä. Sillä hetkellä, kun presidentti Vladimir Putin alkoi julkisesti nöyryyttää joitakin ylempiä johtajiaan – tiedustelupalvelunsa johtajaa Sergei Naryshkinia ja myöhemmin puolustusvoimien komentajaa, kenraali Valeri Gerasimovia – tarvittava organisaation sisäinen luottamus saattoi rikkoutua, ja organisaatio palasi vähemmän ennakoivaan "noudata vain käskyjä" -tilaan välttääkseen lisää nöyryytyksiä. Tämä ei ainoastaan vähentänyt sotilaallista tehokkuutta, vaan myös käynnissä olevien hybridioperaatioiden tehokkuutta länttä vastaan.

ELEKTRONISEN SODANKÄYNNIN PUUTE: JOHTUVATKO ONGELMAT VENÄJÄN OMAISTA VIESTIYHTEYKSISTÄ?

Sen jälkeen kun Venäjän armeija oli käyttänyt intensiivisesti elektronisen sodankäynnin kyvykkyyksiä (esim. taajuuksien häirintää tai elektronisten laitteiden, kuten GPS-laitteiden häirintää) viimeisten kahdeksan vuoden aikana Donbassin / Luhanskin alueella, länsimaista sotilaallisen kyberalueen määritelmää laajennettiin äskettäin kattamaan myös elektroninen sodankäynti. Siksi länsimaiset sotilasasiantuntijat olettivat, että Venäjän sotilasoperaatioihin Ukrainassa liittyisi raskasta elektronista sodankäyntiä, jota oli jo osoitettu Donbassissa ja Luhanskissa. Mutta näin ei tapahtunut. Länsimaisten asiantuntijoiden keskuudessa kiertää erilaisia selityksiä elektronisen sodankäynnin toiminnan puuttumiselle tai puutteelle.

Näyttää siltä, että Venäjä on kamppaillut häirintätaajuuksien välisen kompromissin ja omien joukkojensa komennon ja valvonnan säilyttämisen tarpeen kanssa käyttämällä näitä taajuuksia sekä niin sanotun "viimeisen mailin" ongelman kanssa, joka koskee liikkuvien eteenpäin sijoitettujen joukkojen tukemista digitaalisella datalla. Näyttää siltä, että Venäjän joukot ovat ohittaneet ongelman käyttämällä Ukrainan viestintäverkkoja.

Ukrainalaiset tiedustelulähteet ovat julkaisseet paljon venäläistä sotilasviestintää, jota on siepattu ukrainalaisten verkkojen ja internetyhteyksien kautta. Mikä tietysti estää venäläisiä komentajia antamasta käskyjä sulkea nämä verkot elektronisen sodankäynnin avulla, sillä venäläiset tarvitsevat verkkoa myös itse.

Kyber-potentiaali vastaa osaltaan perinteistä sotilaallista voimaa. Kybertoimintaympäristön osat lisäävät konfliktiin aivan uuden ulottuvuuden. Hakkereiden lisäksi näemme ennennäkemättömän määrän avointen lähteiden tiedustelua kännykkävideoiden kautta sekä kilpailun meemien ja vaihtoehtoisten narratiivien

Lähteet sivulla 15

kautta kaikissa sosiaalisen median kanavissa. Kyberistä, mukaan lukien tietotekniikka ja informaatioalue, on tullut yhtä merkittävä voima kuin sotilaallisesta voimasta. Vaikka Ukraina on voittamassa meemien ja narratiivien sodan Venäjää vastaan, erityisesti länsimaisella ja kansainvälisellä rintamalla, on edelleen vaikea arvioida ulkopuolelta, missä määrin Ukrainan vastanarratiivit voivat tavoittaa tai vaikuttaa Venäjän väestöön, johon vaikuttavat valheelliset narratiivit "denatsifikaatiosta" ja "kansanmurhan estämisestä".

Lisäksi voimme havaita eräänlaista sovellettua "hybridiajattelua" Venäjän asevoimien salaisessa käytössä Valko-Venäjällä ja oletettavasti Luhanskissa sijaitsevia kohteita vastaan Valko-Venäjän ja separatistien tuen varmistamiseksi. On liian aikaista arvioida hakkerien vaikutuksia. Sen jälkeen, kun Ukraina keräsi "30 000 hakkerin armeijan" ja kun Anonymous asettui Ukrainan puolelle, ei ole täysin selvää, mitä verkoissa tapahtuu. Kybertoimintaympäristössä on vilkasta toimintaa, mutta on vaikea arvioida, onko Ukraina vahvistanut tietoturvaansa riittävästi jatkuvan hyökkäyksen vuoksi, tarvitsevatko Venäjän joukot edelleen pääsyä internetiin ensisijaisena viestintävälineenä tai neutralisoiko Anonymous venäläisiä trollitehtaita.

Venäjän hyökkäys, jota kutsutaan vain "sotilaalliseksi erikoisoperaatioksi", Ukrainaan 24. helmikuuta 2022 on ymmärrettävä hybridisodaksi, joka eskaloitui liian pitkälle. Venäjän aktiviteetteja sodan alkuvaiheen epäonnistumisen jälkeen on analysoitava ja käsiteltävä myös osana tavanomaista sotateoriaa eikä vain osana "hybridisodan" teoriaa.

Venäjän asevoimien toiminta ja erityisesti sen tehtävätaktiikka eivät ole täyttäneet edes aseellisia konflikteja koskevien humanitaaristen lakien asettamia kansainvälisiä perusnormeja. Tämä lisää organisatorisen tai systeemisen ulottuvuuden yksittäisten sotilaiden havaitsemien tapahtumiin, jotka täyttävät sotarikosten tunnusmerkistön.

HYBRIDISODASTA TAVANOMAISEEN SOTAAN

Kun alkuperäinen hybridilähestymistapa, jossa maavoimia käytettiin Ukrainan hallituksen pakottamiseen, oli epäonnistunut ensimmäisen kymmenen päivän aikana, Venäjän asevoimat ryhmittyivät uudelleen, hyödyntäen myös heille turvallista Valko-Venäjän aluetta. Länsimaisten tarkkailijoiden suureksi yllätykseksi Venäjä alkoi tämän jälkeen omaksua toisen maailmansodan kaltaisen kulutussodankäyntiin perustuvan hyökkäystyylin 21. vuosisadan länsimaisen modernin sodankäyntikonseptin sijaan, joka perustuu tarkkuusohjattuihin ampumatarvikkeisiin siviiliuhrien vähentämiseksi. Tämä on tehnyt Venäjän operaatioista julmia ja aiheuttanut siviiliuhrien lisäksi raskaita sotilasuhreja Ukrainan asevoimille.

Strategian nimissä harjoitetun brutaalin ja liiallisen sotilaallisen voimankäytön, jota asiantuntijat ovat nimittäneet myös ”terrorismiksi, lisäksi Center of Excellence Countering Hybrid Warfare Community of Interest for Strategy and Defense havaitsi myös hybridisodankäynnin arsenaaliin kuuluvien sodan kynnyksen alapuolella sovellettavien sotilaallisten menetelmien käyttöä Ukrainassa. Täitä ovat esimerkiksi systeemisten haavoittuvuuksien maalittaminen ja niihin hyökkääminen, pyrkimyksenä vaikuttaa päätöksentekoon tai heikentää ja terrorisoida Ukrainan yhteiskuntaa.

Sotilaskohteiden lisäksi Venäjän joukot ja sen alaiset toimijat ovat alkaneet kohdistaa iskuja yhteiskuntajärjestelmän kannalta kriittisiin kohteisiin Ukrainassa. He ovat toteuttaneet tahallisia ja toistuvia hyökkäyksiä tärkeisiin rautatieinfrastruktuureihin ja sähköverkon solmukohtiin. Nämä hyökkäykset sopivat hybridisodan määritelmään sekä määritelmään, jota kutsutaan poikkileikkaavaksi vaikuttamiseksi (cross-domain effects) länsimaisessa sotilasterminologiassa. Yhteenvetona voidaan todeta, että Venäjä on soveltanut sodankäyntikykyynsä kokonaisvaltaista järjestelmäajattelua, mikä mahdollistaa monimutkaisemmat sotilasoperaatiot.

Siinä missä ukrainalainen rautatiejärjestelmä on osoittautunut erittäin kestäväksi,[2] Ukrainan sähköjärjestelmä, oletettavasti olennaisen infrastruktuurin ja kriittisten varaosien koon ja tarpeen vuoksi, on säännöllisesti kärsinyt voimakkaasti ohjusiskuista ja pitkäkestoisemmista sähkökatkoksista.

Venäläiset disinformaatioasiantuntijat ovat vuosien varrella yrittäneet vaikuttaa Ukrainan väestöön "kohdennetulla viestinnällä". Ponnistelut ovat kuitenkin olleet turhia niiden informaatioarvon kalvetessa Venäjän joukkojen esimerkiksi Butšassa toteuttamien sotarikosten rinnalla. Siitä huolimatta Venäjän propaganda, joka viestii "pahoista ukrainalaisista", on ollut jatkuvasti menestyksekästä Venäjän väestön keskuudessa. Internet-kyselyt osoittavat edelleen venäläisten empatian tai sympatian täydellistä puutetta ukrainalaisia kohtaan. [4]

Vaikka monet länsimaiset tarkkailijat olivat yllättyneitä siitä, miten Venäjä toteuttaa sotilasoperaatioitaan, kaikki nämä esimerkit liittyvät syvästi toisiinsa ja juurtuvat sen teoreettiseen sotilaalliseen ja strategiseen ajatteluun. Venäjän ajatusta refleksiivisen kontrollin teoriasta sovelletaan kuitenkin ensimmäistä kertaa samalla tavalla ja rinnakkain sodan kynnyksen alapuolella olevissa hybridisodankäyntiympäristöissä ja todellisissa sotaympäristöissä samanaikaisesti; se tapahtuuko tämä vahingossa tai tarkoituksella nähdään sodan jälkeen.

REFLEKSIIVINEN KONTROLLI

"Refleksiivinen kontrollointi on toimintaa, joka vaikuttaa vastustajan päätöksentekoprosesseihin tarkoituksenmu-

kaisesti muunnellulla tiedolla valmistellussa informaatiokampanjassa. Tällaisen väärennetyn informaation ensisijainen tavoite on saada toinen osapuoli tekemään päätöksiä, jotka itse asiassa ovat tiedon tuottajan ennalta määräämiä." [6]

Refleksiivisen kontrollin käsitteellä on pitkä historia Venäjän sotilasstrategioissa. Sitä opetetaan sotilaskouluissa ja akatemioissa, ja se on myös kodifioitu Venäjän kansalliseen turvallisuusstrategiaan.

Sen osia ovat:

- Voimankäytön uhka (provokaatio ja pelote);
- Mis- ja disinformaation välittäminen (valheet ja huomion siirtäminen);
- Vihollisen päätöksentekoalgoritmiin vaikuttaminen (uuvuttaminen, jakolinjojen luominen ja painostaminen); ja
- Päätöksentekoaikaan vaikuttaminen (hidastaminen ja ylikuormitus). [7]

Venäjän refleksiivisen kontrollin perusta ulottuu yli 200 vuoden taakse. Se seuraa kenraali Peter Rumyantsevin (Ajatuksia) ja Alexander Suvorovin (Voiton tiede) ajatuksia. [8] Kaiken kaikkiaan refleksiivinen kontrolli noudattaa löyhästi tunnetun kiinalaisen kenraalin Sun Tzun sodankäynnin teoriaa: "Sodan korkein taito on alistaa vihollinen taistelematta". Sitä on myöhemmin päivitetty mm. Evgeny Messnerin 1920-luvun lopun ajatuksilla kumouksellisesta sodasta, toiminnasta, jonka tarkoituksena on heikentää vastustajan sosiokulttuurista ja sotilaallista yhteenkuuluvuutta. Kuten myös Alexander Duginin ajatuksilla verkkokeskeisestä sodasta, joka tapahtuu virtuaalisessa ulottuvuudessa, jossa kontrollia luodaan enemmän poliittisessa mielessä kuin sotilaallisessa (ei pidä sekoittaa länsimaisiin ajatuksiin verkkokeskeisestä sodankäynnistä). Myös Igor Panarinin ajatuksilla informaatiosodankäynnistä, sen psykologisesta ja informaatiovaikutuksista on hyödynnetty. Kaikkia informaatiokeinoja käytetään päätöksentekoprosesseihin vaikuttamiseen manipuloimalla kansainvälistä ja kotimaista yleistä mielipidettä. [9]

MODERNIN TEKNOLOGIAN HYBRIDIKÄYTTÖ

Ihmiskunnan alusta lähtien sota on ollut säälimätön uudistaja, eikä Venäjän sota Ukrainaa vastaan tee poikkeusta tähän sääntöön.

Kyber

Ukrainan IT-järjestelmät ovat Venäjän jatkuvien hyökkäysten kohteena. Kyberhyökkäykset ovat myös osa tavanomaista sodankäyntiä. Toisaalta hyökkäävien kyberoperaatioiden niin sanottuja heijastus- tai dominovaikutuksia – joita länsimaiset asiantuntijat ennustivat argumentoidessaan hyökkäävien sotilaallisten kyberoperaatioiden käyttöä vastaan – ei toistaiseksi ole havaittu. Johtopäätöksenä on todettava, että kriittiset infrastruktuurit on tunnistettava varhaisessa vaiheessa ja suojattava sekä niitä on pystyttävä puolustamaan fyysisesti että kyberympäristössä samanaikaisesti.

HYBRIDIUHAT JA SODANKÄYNTI UKRAINAN ULKOPUOLELLA

Ukrainan sotaan liittyy Venäjän strategiset hybridioperaatiot. Venäjä soveltaa lähes kaikkia edellä mainittuja keinoja ja menetelmiä myös muissa operaatioissa ympäri maailmaa:

- Venäjän yksityiset sotilasyritykset (PMC) toimivat Afrikassa yhtä raa'asti kuin Ukrainassa, mutta lähes ilman rektioita kansainväliseltä yhteisöltä. Se, että Wagner-palkkasoturit ja Malin armeijan yksiköt tappoivat 300 malilaista siviiliä, ei aiheuttanut juuri mitään kansainvälistä reaktiota [10]
- Venäjällä on käynnissä pysyviä disinformaatiokampanjoita ennalta perustettujen verkostojen kautta kaikkialla Euroopassa ja Amerikassa
- Niin sanottujen "hyödyllisten idioottien" ja vaikuttajien käyttö on helppoa lähes kaikissa länsimaisissa yhteiskunnissa
- Kriittisiin infrastruktuureihin kaikkialla Euroopassa kohdistetaan hyökkäyksiä, joissa syyllistä ei ole joko voitu osoittaa tai Venäjä on pystynyt peittämään ja kieltämään osallisuutensa
- Kyberhyökkäykset länsimaisia poliittisia johtajia vastaan, erityisesti niitä, jotka ovat julkisesti tukeneet Ukrainaa ja sitoutuneet taisteluun Venäjää vastaan.

TAISTELUARVO = KYVYT X MOTIVAATIO²

Länsimaiset asiantuntijat puhuvat pääasiassa teknologiasta sotilaallisen voiman tai vallan liikkeellepanevana voimana. Sotilasjohtajille opetetaan kuitenkin jo hyvin varhaisessa vaiheessa uraansa, että heidän joukkojensa taisteluarvo on nähtävä näiden kykynä (tekniset keinot/aseet) suorittaa tehtävä kerrottuna heidän joukkojensa motivaation neliöllä.

Normaalisti tämä näkyy vain yksittäisten joukkojen tasolla, mutta Venäjän sota Ukrainassa osoittaa, että tätä on tarkasteltava myös laajemmalla tasolla. Se selittäisi, miksi Ukrainan armeija ja heidän "vapaaehtoiset taistelijansa" voivat menestyksekkäästi kohdata mahtavaksi arvioidun Venäjän sotavoiman.

Venäjän maavoimien heikko henkinen valmistautuminen, joka johti sotilaskarkureihin ja kaluston hylkäämiseen, voidaan tulkita myös merkiksi siitä, että erityisesti Venäjän sotilasjohto on saattanut nähdä

Lähteet sivulla 15

sodan käymisen vain yhtenä mahdollisena vaihtoehtona hybridioperaatiossa Ukrainaa vastaan, ja siksi suunnittelu oli puutteellista.

Venäläiset naamioivat ensimmäiset päähyökkäyksensä Ukrainaan - Kiovaan pohjoisesta, Donbasiin/Luhanskiin idästä ja Mariupoliin etelästä käyttämällä pataljoonatason iskujoukkoja ilman logistista- tai viestinnälistä tukea, mikä aiheutti ongelmia länsimaisille tiedustelupalveluille, jotka yrittivät arvioida Venäjän aikomuksia. Ukrainan onneksi joukkojen keskittäminen ei sujunut suunnitellusti ja Venäjän joukot ovat kärsineet viestinnän ja logististen järjestelyjen puutteesta tai toimimattomuudesta. Myös joukkojen alhainen moraali on vaikuttanut, sillä Valko-Venäjältä ennen hyökkäystä saatujen raporttien mukaan venäläiset yksiköt olivat joutuneet raivaamaan metsää polttopuiksi ja ostamaan ruokaa omilla rahoillaan ja luulivat olevansa vain harjoituksessa.

MITÄ UUTTA VENÄJÄN SOTA JA SODANKÄYNNIN MENETELMÄT TUOVAT HYBRIDISODANKÄYNTIIN JA HYBRIDIUHKIIN

Venäjän asevoimat, salaiset palvelut ja PMC:t ovat valmiita käyttämään epäinhimillistä julmuutta ja väkivaltaa jopa julkisesti. Länsimaiset oletukset siitä, että Venäjä tai venäläiset toimijat eivät moraalisyistä suorittaisi salaisia operaatioita, joissa toteuttajan tunnistaminen on lähes mahdotonta, tulisi unohtaa.

Kirjoittajat suhtautuvat skeptisesti siihen pystyvätkö länsimaiset armeijat, kuten NATO-liittolaiset, luomaan oikean tilannekuvan ja uusia sodankäynnin konsepteja, kuten "kognitiivisen sodankäynnin käsitteen". Käsitteen, joka pystyy selviytymään Venäjän refleksiivisen kontrollin teoriasta. Kopioimalla jälkimmäinen saavutettaisiin vain arvopohjainen sotajoukko, jonka avulla ei estää Venäjän ulkopuolisen vaikuttamisen kyvykkyyttä sen koko laajuudessaan. Lisäksi Venäjä on soveltanut systeemiajattelua sekä hybridi- että perinteisessä sotilaallisessa doktriinissaan ja pystyy toteuttaa sotilasoperaatioita sen mukaisesti.

Tämä korostaa kykyä toteuttaa nopeasti monialaisia operaatioita ja ajatella puolustusta uudelleen kokonaispuolustuksena integroimalla ei-sotilaalliset turvallisuustoimijat ja pyrkimällä yhteiskunnalliseen kriisin kestävyyteen.

Viime vuoden aikana asiantuntijat ovat jatkuvasti analysoineet ja keskustelleet mahdollisista skenaarioista Venäjän Ukrainaa vastaan käymän sodan lopputuloksesta. Yksi yhteinen piirre kaikissa skenaarioissa on ollut, että hybridisodankäynti jatkuu niiden halvan ja valitettavasti tehokkaan sekä joustavan luonteen vuoksi. Venäjän armeijan odottamattoman suuret tavanomaiset henkilöstö- ja materiaalimenetykset lisäävät hybridiuhkien riskejä sodanjälkeisessä turvallisuusympäristössä.

Voitti tai hävisi Venäjä sodan, sillä on tarve tavanomaisen sotilaallisen voiman kehittämiseen sekä uudelleen organisointiin. Tänä väliaikana hybridivaikuttaminen uhat ja -sodankäynti ovat Venäjän ensimmäinen ja halvin vaihtoehto vaikuttamiseen, erityisesti Euroopan geopoliittisella alueella. ■

DR. JOSEF SCHRÖFL

- Kandidaatin tutkinto tietotekniikassa ja maisterin tutkinto kansainvälisistä suhteista Delawaren yliopistosta. Tohtorin tutkinto kansainvälisestä politiikasta Wienin yliopistosta.
- Strategiasta ja puolustuksesta vastaava apulaisjohtaja.
- **Hybrid CoE Helsinki/Suomi**

SOENKE MARAHRENS

- Tietojenkäsittelytieteen tutkinto sekä maisterin tutkinnot Royal Military Collegesta, Kanadasta ja Federal Armed Forces -yliopistosta, Hampurista.
- Johtaja, strategia ja puolustus, johtaa hybridisodankäynnin tutkimushaaraa.
- **Hybrid CoE Helsinki/Suomi**

LÄHTEET :

[1] Lonas Lexy, “Here are Russia’s alleged war crimes in the Ukraine invasion,” The Hill, https://thehill.com/policy/international/3262626-here-are-russias-alleged-was-crimes-in-the-ukraine-invasion/.

[2]Jack Peat, “War-torn Ukraine running more reliable train service than TransPennine Express,” January 06, 2023, https://www.thelondoneconomic.com/news/war-torn-ukraine-running-more-reliable-train-service-than-transpennine-express-342002/.

[3] Claire Parker, “Russia and Syria conducted dozens of illegal ‘double tap’ strikes, report says,“ The Washington Post, https://www.washingtonpost.com/world/2022/07/21/syria-russia-double-tap-airstrikes-report-war-crimes/.

[4] Lew Gudkov, “Interview Conducted by Christina Hebel in Moscow,” Der Spiegel, https://www.spiegel.de/international/world/opinion-researcher-lev-gudkov-russians-have-little-compassion-for-the-ukrainians-a-066c08c6-60f4-48e1-853a-d2b3d67bd6b8.

[5] The initial assumption about the trustworthiness of the mercenaries was already raised during the Webinar on 14.02.2023.

[6] ”Seeing Red,” Hybrid COE 8th Research Report, Jukka Aukia & Lucjan Kubica, March 2023, 34.

[7] Former Research Director of Hybrid COE, Prof Dr Hanna Smith, in a “mind-opening” email exchange with the author.

[8] Former Research Director of Hybrid COE, Prof Dr Hanna Smith, in a “mind-opening” email exchange with the author.

[9] Former Research Director of Hybrid COE, Prof Dr Hanna Smith, in a “mind-opening” email exchange with the author.

[10] Emmanuel Akinwotu, April 05, 2022, “Russian mercenaries and Mali army accused of killing 300 civilians,” https://www.theguardian.com/world/2022/apr/05/russian-mercenaries-and-mali-army-accused-of-killing-300-civilians.

KRIISIVIESTINTÄ VAHVISTAA RESILIENSSIÄ

// Taneli Hassinen

Kriisiviestinnällä pyritään lievittämään kriisin vaikutuksia sen osallisiin ihmisiin. Tavoitteena on kommunikoida tilannekuvasta käsin kriisin skenaarioita sekä sitä, mitä tilanteen korjaamiseksi tehdään.

Kriisi järkyttää tavalla tai toisella ihmismieltä. Iso kriisi suuresti, pieni kriisi vähemmin. Jokaisella on kriisiin oma henkilökohtainen suhteensa. Kriisiviestinnällä annetaan ihmisille materiaalia ja käsitteitä työstää kokemaansa sekä palauttamaan normaalitila niin pian kuin mahdollista.

Kriisejä on monenlaisia. Onnettomuus on yksi tyypillisimpiä kriisitilanteita. Kriisiviestinnän tarve syntyy vasta, kun sen vaikutukset alkavat koskea yksilöitä tai kokonaisia sidosryhmiä. Siihen asti kyse on kriisijohtamiseen liittyvistä informaatiovirroista ja niihin perustuvasta päätöksenteosta, ehdottoman tärkeitä nekin.

Kriisiviestintää aletaan tehdä siinä vaiheessa, kun ihmisten ajatteluun, kokemukseen ja toimintaan halutaan vaikuttaa. Silloin osallisilla ovat pelissä emootiot, arvot ja uskomukset. Niihin pyritään vaikuttamaan tilannekuvaa hahmottamalla sekä faktoja tarjoamalla, mutta myös kohtaamisen kokemuksella, sillä se vahvistaa kriisiviestinnästä vastaavan eetosta – tai heikentää sitä.

Tässä tullaan kriisiviestinnän ytimeen. Se on viime kädessä turvallisuuden ja hallinnan tunteiden eli osallisten toimijuuden vahvistamista. Tämän päällä lepää yksilöllinen ja kollektiivinen resilienssi. Ongelmatilanteita ratkotaan osana kriisijohtamista, mutta kriisin arvaamattominta lenkkiä, ihmistä, ohjataan oikeanlaisella viestinnällä.

KYBERISSÄ PUHUTAAN IHMISTEN PERUSTARPEISTA

Toisen merkittävän kriisien ryhmän muodostavat elinoloihin vaikuttavat kriisit. Niitä ovat poikkeukselliset luonnonilmiöt, jotka vaikuttavat infrastruktuuriin, erilaisiin järjestelmiin. Toisaalta myös tartuntataudit voivat laittaa yhteiskunnan järjestelmät ja toimijat polvilleen, kuten olemme perusteellisesti saaneet oppia.

Kybertodellisuus on moderneille ihmisille elinympäristö ja olosuhde. Siihen tulevat häiriöt vaikeuttavat nopeasti ihmisten arkeen suoraan sekä yhteiskunnan erilaisiin infroihin, kuten sähkö, vesi, ruoka, raha ja liikenne.

Häiriö voi tulla erilaisista virheistä tai onnettomuuksista, mutta erityisesti viime aikoina on järjestelmille alettu aiheuttaa ongelmia myös tarkoituksellisesti. Käynnissä oleva maailmanpoliittinen jännite tuottaa toimijoille tarvetta särkeä toisten elämänoloja.

Riippumatta aiheuttajasta häiriöt ja niiden uhat palauttavat ihmiset perustarpeiden äärelle. Tarvehierarkian alalauteilla ovat välittömiin elintoimintoihin ja fyysiseen hyvinvointiin liittyvät tarpeet. Seuraavana on turvallisuus ja koskemattomuus.

Näiden tarpeiden tyydyttäminen synnyttää välittömästi kirjon erilaisia ajatuksia ja emootioita, joita kriisiviestinnällä pyritään ohjaamaan. Puhumattakaan hienostuneemmista tarpeista, kuten yhteenkuuluvuus, omanarvontunto ja itsensä toteuttaminen. Kaikkia näitä voidaan häiritä.

KRIISIVIESTIJÄN KOKO OLEMUS ON VIESTI

Vaativassa kriisiviestinnässä eivät riitä pelkät faktat. Ne ovat luonnollisesti välttämätön työkalu. Ihmisen päätöksentekoon vaikuttavat tutkitusti hänen emootionsa enemmän kuin olemme useinkaan valmiita uskomaan. Faktojen fraktioita sijoitetaan emootiopohjaan paljolti sen pohjalta, miten faktojen tarjoajaan luotetaan.

Kyse on siis klassisesta retoriikan elementistä ethoksesta. Kaksi muutahan ovat logos (sanat ja logiikka) ja pathos (tunne). Eetos ilmenee vahvimmillaan viestijän olemuksesta eli kehonkielestä, joissa muun muassa ilmeet ovat ratkaisevia. Suuri osa ihmisen kehonkielestä nousee tiedostamattomasta, joten se paljastaa puhujansa arvomaailman ja uskomusjärjestelmänsä. Siksi mielen sisuskalut on oltava kunnossa.

On selvää, että viranomaisviestijältä odotetaan toisenlaista olemusta ja kehonkieltä, kuin vaikkapa kriisin kohteeksi joutuneen organisaation edustajalta, joka organisaationsa kriisitoimien johtajana saattaa olla myös uhri.

Myös huolenpidon muoto voi kaupallisella toimijalla olla toinen kuin viranomaisella. Kriisiin joutunut ihminen odottaa aina kuitenkin välittämistä ja sen ilmaisua sanallisesti ja olemuksellisesti. Se nousee meidän psyykkisestä rakenteestamme.

MEDIA EDUSTAA TIEDONJANOISTA YLEISÖÄ

Kriisiviestinnässä keskeisessä roolissa on media – niin toimitettu kuin sosiaalinenkin. Nykyisin viestivällä organisaatiolla on käytössään omia digitaalisia kanaviaan, erilaisia some-tilejä ja oma verkkosivustonsa. Niiden aktiivisuus ja relevanttius ohjaa yleisöä myös niiden pariin.

Suuremmissa tai dramaattisemmissa kriiseissä myös perinteinen media muodostaa tilanteesta journalistisen näkemyksensä. Ihmisiä koskevissa kriiseissä media seuraa kriisin ytimessä olevaa emootiota. Se on sen tehtävä. Siksi myös kriisiviestijän tulee ymmärtää emootioiden logiikkaa ja vaikuttaa emootioiden todellisuuteen.

On aina parempi, jos relevantteihin medioihin ja toimittajiin on luotu taustoittavat suhteet jo ”rauhan aikana”. Silloin helpompi kriisin keskellä saada mediassa läpi oikeaa ja valistunutta tietoa.

Mainetta ei voi hallita, mutta sen muodostaviin tekijöihin voi pyrkiä vaikuttamaan osaavalla kriisiviestinnällä. Organisaation maine yleisön keskuudessa muodostuu jokaisen yksilön päässä. Toki se joukkoistuu, missä kaikkinainen media toimii alustana.

KRIISI ON EPÄNORMAALI TILA

Kriisi on sen kokijalle aina normaalista poikkeava tilanne. Muutenhan se ei olisi kriisi. On normaalia, että kriisissä oleva ihminen kokee epänormaaleja tunteita. Tilanteesta pyritään pois kohti normaalia elämää mahdollisimman vähin traumoin.

Kriisiviestintä on itsensä ja muiden toimijoiden mielensisäisen maailman tuntemista ja siihen vaikuttamista. Sitä pitää harjoitella ennen kuin kriisi iskee. Sanoituksia pitää hioa, esiintymistä kameran edessä toistaa. Silloin toimiminen kriisiviestintätilanteissa on luontevampaa.

Kriisiin voi valmistautua. Kriisiviestinnän periaatteet, roolitukset – ennen kaikkea johtovastuu – ja ohjeistukset ovat välttämättömiä. Niiden puuttuminen on sulaa hölmöyttä. Potentiaalisten poikkeustilanteiden skenarointi helpottaa merkittävästi kriisiviestinnän käynnistämistä tilannekuvan tarkennuttua.

Kriisijohtamisessa pyritään ratkaisemaan itse ongelmaa. Kriisiviestinnällä pyritään samaan sosiaalinen hyväksyntä toimille, selvitä mahdollisimman pienin mainekolhuin ja vahvistaa kaikkien osallisten resilienssiä. ■

TANELI HASSINEN

Taneli Hassinen on toiminut viestintäjohtajana Finnairissa, SRV:ssä ja Taalerissa. Viime vuodet hän on toiminut Functos Oy:ssä mm. kriisiviestinnän konsulttina.

TIETOVUOTOJEN TALOUDELLISET VAIKUTUKSET

// Leo Taalas

Digitaalinen murros on tuonut hyötyjä ja luonut merkittäviä riskejä ja haavoittuvuuksia. Tietomurrot ovat viime vuosina lisääntyneet voimakkaasti, kun digitaaliset järjestelmät ovat lisänneet hyökkäyspintaa. Tietojen turvallisesta hallinnasta on tullut strateginen haaste yrityksille, jotka käyttävät digitaalisia työkaluja. Kyberhyökkäyksiä vastaan valmistautumisesta on tullut yritysten strateginen huolenaihe.

Yrityksen prosesseja, asiakkaita tai työntekijöitä koskevien arkaluonteisten tietojen vuotaminen vaikuttaa kielteisesti yrityksen päivittäiseen toimintaan, palveluihin ja tuloihin. Julkinen ilmoitus tietomurron kohteeksi joutumisesta voi myös vaikuttaa maineeseen ja osakekurssiin. Ilmoituksella voi olla vaikutuksia myös yrityksen julkisuuskuvaan, suhteisiin alihankkijoihin, asiakkaisiin ja työntekijöihin. Ilmoituksen taloudellisten vaikutusten arvioiminen onkin hankalaa.

Kiinnostus kyberhyökkäysten taloudellisiin vaikutuksiin heräsi vuoden 2001 syyskuun 11. päivän hyökkäysten jälkeen. Mike McConnell, Yhdysvaltain kansallisen turvallisuusviraston entinen johtaja, varoitti mahdollisesta "Cyber 9/11" -tapahtumasta mahdollisena jatkona fyysiseen hyökkäykseen. Laajamittaisen kyberhyökkäyksen mahdollinen uhka johti tutkimukseen, jolla selvitettiin hyökkäysten merkitys yrityksille.

Suuri osa kyberhyökkäysten vaikutuksia yrityksiin käsitelleistä tutkimuksista on käyttänyt tapahtumatutkimusmetodologiaa. Yleensä aikaisemmat tutkimukset ovat odotetusti löytäneet negatiivisen korrelaation kyberhyökkäysten ja osakekurssien välillä. Viime aikoina kyberhyökkäysten vaikutuksia on analysoitu myös eri toimialoilla ja ajankohtina.

Bocconin yliopistoon kesällä 2023 tekemässäni opinnäytetyössä sovelsin markkinamallin tapahtumatutkimusta – tapahtumatutkimuksen metodologian muunnelmaa – arvioidakseni ilmoitettujen tietomurtojen vaikutuksia yhdysvaltalaisiin osakekursseihin. Käytetty malli ennusti odotetun pörssikurssin käyttäen 135 päivän jaksoa ennen tietomurron julkistamista. Käyttäen ennustettua pörssikurssia, arvion 1-20 päivän tapahtumanikkunassa kumulatiivista epänormaalia tuottoa (CAR) sekä sen avulla kumulatiivista keskimääräistä epänormaalia tuottoa (CAAR).

Mallinnus perustui aineistoon, jonka kokosin yhdysvaltalaisen Privacy Rights Clearing Housen (PRC) tietoloukkausten kronologiasta. Siihen valittiin hakkeroinnin vuoksi tietomurtojen kohteeksi joutuneita julkisesti noteerattuja yrityksiä. Aineisto koostui 63 tietomurtotapahtumasta ajalta 2.1.2005–2.7.2022. Tutkimuksessa käytetyt NASDAQ- ja NYSE-osake- ja indeksihinnat kerättiin Refinitiv DataStreamista (Datastream International, 2023).

Analyysi vahvisti odotetusti aikaisemmissa tutkimuksissa löydetyn negatiivisen kumulatiivisen keskimääräisen epänormaalin tuoton (CAAR) tietomurtoilmoitusten jälkeen. Tulokset osoittavat koko aineistolla suurimman negatiivisen kumulatiivisen keskimääräisen epänormaalin tuoton (CAAR) -1,8 % kolme päivää tietomurtoilmoituksen jälkeen.

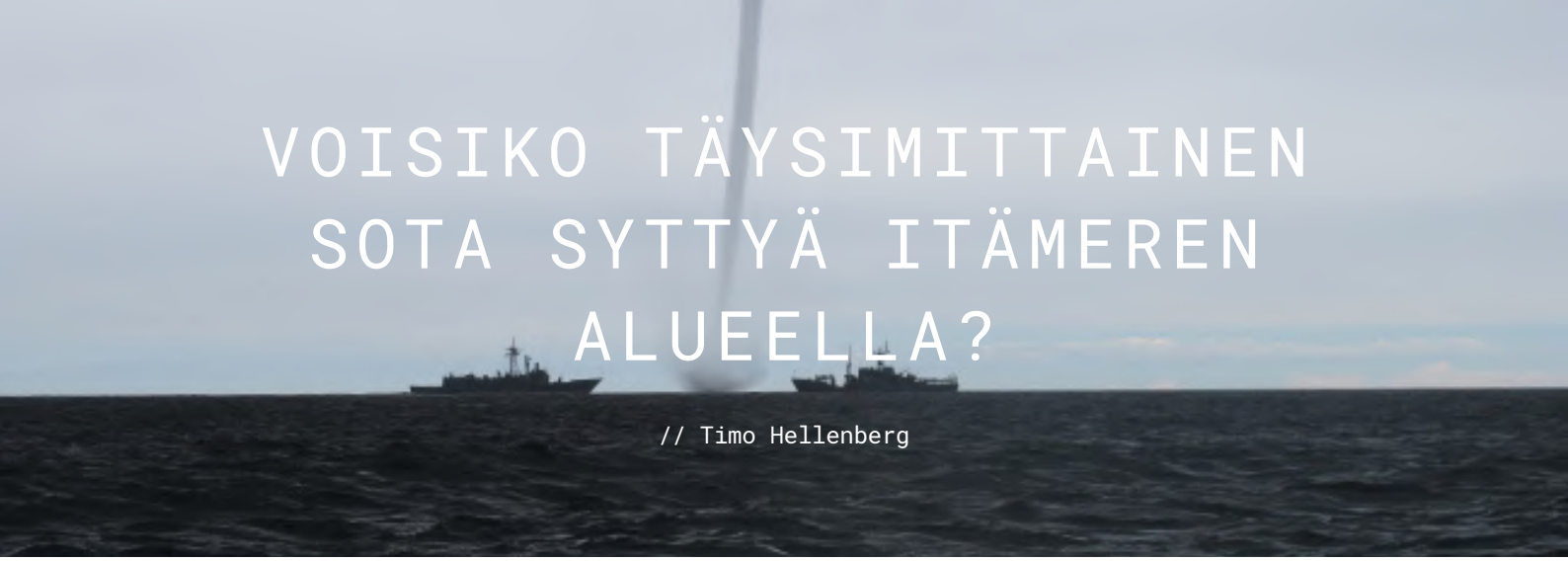
Toiseksi arvioin NASDAQin ja NYSE:n pörssiyhtiöiden välistä eroa. NYSE:n listatuissa pörssiyhtiöissä tietomurtoilmoitus aiheutti -1.3 % CAARin kaksi päivää ilmoituksen jälkeen, vastaavasti NASDAQ-listatuissa yhtiöissä vaikutusta ei havaittu tilastollisesti merkitseväksi. Tuloksen voi selittää markkinoiden toiminnallinen ero tai listattujen yhtiöiden luonne. Aihe vaatii lisätutkimuksia.

Kolmanneksi analysoin eroja tietomurtoilmoitusten vaikutuksissa osakkeiden hintaan toimialojen välillä. Suurin vaikutus löytyi rahoitussektorilta, jossa CAAR oli negatiivinen -1,3 % kaksi päivää ilmoituksen jälkeen. Vähittäiskauppassa negatiivinen vaikutus oli huomattavasti pienempi -0,43% mutta se seurasi välittömästi ilmoitusta. Tulokset eivät viitanneet tietomurtoilmoitusten merkittävään vaikutukseen teollisessa tuotannossa tai teknologiayrityksissä. Tosin ryhmien heterogeeninen luonne voi heikentää analyysin tuloksia tältä osin. Voimakkaampi reaktio tietomurroihin finanssisektorilla johtuu todennäköisesti luottamuksen keskeisestä roolista finanssiyritysten liiketoimintamallissa.

Tulokset antavat viitteitä tietomurtojen vaikutuksista pörssikursseihin ja kannustaa jatkotutkimuksia. Tietomurrot ovat yrityksille vakava uhka, joihin tulee varautua. ■

LEO TAALAS

Analyytikko
Cyberwatch Finland



VOISIKO TÄYSIMITTAINEN SOTA SYTTYÄ ITÄMEREN ALUEELLA?

// Timo Hellenberg

Venäjän geopoliittiset tavoitteet Euroopan pohjoisimmilla alueilla ovat kasvussa. Saksan puolustusministeriön vuodetut asiakirjat paljastivat pelottavan uskottavan skenaarion Venäjän täysimittaisesta hyökkäyksestä Baltian maihin ja Puolaan. Raportin mukaan Venäjä voisi mobilisoida jopa 200 000 uutta varusmiestä keväällä 2024, samalla Venäjän armeijan hiljaa kootessa joukkojaan Puolan ja Liettuan rajoille. Ensimmäiset merkittävät Naton joukot saapuisivat Puolaan noin 72 tunnin kuluttua, mutta suuria saksalaisia ja muita eurooppalaisia Naton joukkoja ei nähtäisi ainakaan 10–15 päivään. Kuten Vilnius Security Foorumissa helmikuussa todettiin, tämäkin on myönteinen arvio siitä miten tilanne voi elaboroitua ja aivan ennustamattomasti, kuten Krimin haltuunotto keväällä 2014. Koska Naton pienet valmiusjoukot Baltiassa ovat pitkälti vahvistusten varassa, tilanne on vakava. Suomella ei olisi aikaa mobilisoida tai työntää asevoimien yksiköitään kohti Venäjää, jolloin Venäjä voisi vapaasti pitää sotilasyksikkönsä alueella ennallaan. Saksan haluttomuus sotkeutua tilanteeseen kasvaisi Venäjän ydinkokeen kautta ja ultimaatumilla vastata puuttumiseen Baltian tilanteeseen suoraan ydinasein.

Tässä skenaariossa sota alkaa ensimmäisenä päivänä intensiivisellä ohjustulella arvokkaisiin kohteisiin. Panssarien, rynnäkköhelikoptereiden ja rakettitykistön joukko työntyy Pohjois-Viro-Narvan ja Tallinnan läpi syvemmälle maahan ja samanaikaisesti Viron luoteisrannikkokaupunki Paldiski otetaan haltuun ilmasta ja merellä tulevalla operaatiolla. Samaan aikaan pataljoonan kokoinen merijalkaväki laskeutuu Tallinnan satamaan. Historian havinaa Peipsijärven pohjois ja eteläpuolelta työntyisi maahan panssaroitudut divisioonat, aivan kuten Peipsijärven jäätaistelussa joka käytiin Novgorodin ruhtinaan Aleksanteri Nevskin johtamien novgorodilaisten joukkojen ja saksalaisen ritarikunnan ritareista, Tanskan kuninkaan joukoista ja virolaisista näiden liittolaisista koostuneen sotajoukon välillä 5. huhtikuuta 1242 Peipsijärven rannalla.

Etelässä toinen taso työntyy Valko-Venäjältä luoteeseen kohti Kaliningradin aluetta Liettuan läpi ja kääntyy sitten välittömästi etelään kohtaamaan Puolasta tulevat Naton joukot. Takajoukot tuhoavat Liettuan puolustuksen ja vastarinnan seuraavina päivinä. Latvia jätetään huomiotta ja se jää ikään kuin taskuun Kuurinmaan mottiin. Sen armeijalla ei ole keinoja vastata.

Ennen yllä olevassa skenaariossa kuvattua varsinaista maahyökkäystä venäläiset aloittaisivat hybridivaikuttamiskampanjan, jota voidaan käyttää taloudellisen vaikuttamisen, poliittisen vaikuttamisen, informaatiovaikuttamisen, kybervakoilun ja sotilaallisen vaikuttamisen kautta.

Venäjän strategiset yhdistetyt tai hybridivaikuttamistaktiikat on dokumentoitu hyvin sekä kotimaassaan että lähialueillaan. Uudelle vuosikymmenelle siirryttäessä on selvää, että nämä samat taktiikat ovat löytäneet tiensä Venäjän keinoihin kasvattaa globaalia vaikutusvaltaansa. Yksi suosiotaan kasvattava ase Venäjän työkalupakissa on jatkuvan paineen ylläpitäminen, jota voidaan toteuttaa taloudellisen vaikuttamisen, poliittisen vaikuttamisen, informaatiovaikuttamisen, kybervakoilun ja sotilaallisen vaikuttamisen kautta. Näitä taktiikoita ovat niin ikään etuuskohtelukauppasopimukset, öljyn ja kaasun alennustoimitukset, velkahelpotukset, luotot, korruptoituneen hallituksen ja järjestäytyneen rikollisuuden välinen symbioosi, trollaus ja manipulointi, alueelliset rikkomukset, sotilastiedustelun laajentaminen infrastruktuuriin, avainhenkilöiden "korvamerkitseminen" ja paljon muuta. On tärkeää, että yritykset ja hallitukset ympäri maailmaa pysyvät valppaina näiden taktiikoiden suhteen ja tekevät yhteistyötä niiden vaikutusten lieventämiseksi.

Hälyttävää on, että Venäjän turvallisuuspalvelu on pidättänyt korkean määrän ulkomaalaisia ja Venäjän kansalaisia syytettynä yhteistyöstä ulkomaantiedustelun kanssa sen jälkeen, kun se aloitti hyökkäyksensä Ukrainaan helmikuussa 2022. Tämä toimintatapa voimistuu Venäjän alueilla, joita pidetään uusina herkkinä alueina (новые чувствительные зоны), kuten Baltian maissa ja laajemmassa Karjalassa. Tämä suuntaus kiihtyy mitä syvemmälle Venäjä vajoaa Ukrainan mustaan maaperään. Venäjän tiedustelu on perinteistä ja perustuu ensisijaisesti henkilötiedusteluun ja järjestelmällisiin eliminointeihin. Siinä missä sen vahvuus perustuu henkilötiedustelun

kykyihin ja niin sanottuun ”boots on ground” toimintaan niin sen heikkous piilee sen sektorien välisessä yhteistoiminnassa, koska eri ryhmittymät taistelevat Kremlin suosiosta.

Toinen Euroopan komission tilaama tuore geopoliittinen katsaus viittaa siihen, että tämä voi johtaa alueen hyvinvointiin ja hallintoon kohdistuviin haasteisiin lähivuosina. Suomalaisen tutkimusryhmän Hellenberg Internationalin ja irlantilaisen Munsterin teknillisen yliopiston raportti "Arctic and Security Cooperation - Review of Crisis Coordination and Response Arrangements in the European Arctic and High North" (T. Hellenberg, P. Visuri, S. Milne, 2023) korostaa uusien geostrategisten ja geopoliittisten kitkatekijöiden syntymistä Euroopan pohjoisimmilla alueilla. Itämeri on keskeinen logistinen käytävä, johon kohdistuu paineita.

Hellenberg-MTU:n raportissa korostetaan, että Venäjä on rakentanut nopeasti uudelleen sotilaallisia valmiuksiaan ja nykyaikaistanut alueellista sotilaallista infrastruktuuriaan arktisella alueellaan. Lisäksi Venäjä hyödyntää kaksoiskäyttöä. Tällä tarkoitetaan, että arktista infrastruktuuria käytetään siviili- ja sotilastarkoituksiin ja samalla hyökkäys- ja puolustustarkoitusten välistä rajaa hämärretään. Venäjä on myös kehittänyt Arctic-M-satelliittijärjestelmän valvomaan laajempaa arktista aluetta, kuten Itämerta ja Barentsinmerta. Säätietojen välittämisen lisäksi se välittää myös poikkeustilanteiden tilannetietoja.

Kreml todennäköisesti rohkaisee Pekingin yrityksiä vaikuttaa pohjoisimpien alueiden talouteen ja hallintaan. Arktisen kehityksen pitkän aikavälin rooli Kremlin visiossa on epävarma, erityisesti tulevaisuuden globaalien markkinoiden monimutkaisten skenaarioiden vuoksi. Lyhyen aikavälin ennuste on, että Venäjä todennäköisesti haastaa lännen pohjoisimpien alueiden hallinnassa ja valta-asemassa. Kysymys kuuluu: mikä on Euroopan resilienssi vastata edellä mainittuun haasteeseen, erityisesti tilanteessa, jossa kohtaamme sen ilman itsestäänselvyyksinä pidettyjä liittoutumia?

Kuinka sitten varautua tulevaan? NATO pysyy varmasti Euroopan turvallisuuspilarina myös tulevaisuudessa. Näyttää myös siltä, että erityisesti pienet Itä-Euroopan valtiot ovat vihdoin heräämässä ja panostamassa omaan turvallisuuteensa. Liettua suunnittelee puolustusbudjettinsa kasvattamista 3,5 prosenttiin bruttokansantuotteesta. Mutta ottaako Saksa enemmän vastuuta paitsi omasta turvallisuudestaan myös Itämeren alueen turvallisuudesta? Saksalaisen prikaatin sijoittaminen Liettuaan eteni, kun Saksan puolustusministeri Pistorius vieraili Vilnassa 18.12. allekirjoittamassa etenemissuunnitelman aiheeseen liittyen. Liettuaan siirretään yhteensä 5 000 saksalaista sotilasta ja teknisistä yksityiskohdista sovitaan vuoden 2024 aikana (ml. isäntämaan tukipalvelut, rahoitus ja operaatiot). Prikaatin ytimen muodostavat viisi patal-joonaa panssarivaunu- ja tykistöpataljoonineen. Puolan voimakkaalla kasvulla puolustusmahtina on merkittävä vaikutus koko Baltian turvallisuuteen. Samoin Suomen ja Ruotsin Nato-jäsenyydet luovat pohjan tilanteelle, jossa koko pohjoismaiden alueen turvallisuus on yhden käden ulottuvilla. On kuitenkin tunnustettava, että Natolla – kuten kaikilla hallitustenvälisillä järjestöillä – on omat sisäiset ongelmansa.

Viro, Latvia ja Liettua ovat viemässä sitoumuksensa Itämeren alueellisen turvallisuuden nostamisesta seuraavalle tasolle perustamalla "Baltian puolustuslinjan". Tämä satojen bunkkereiden ja muiden puolustuslaitosten verkosto itärajoilla luo yhteisen puolustusvyöhykkeen ja puitteet asejärjestelmien yhteiskäytölle. Osana tätä hanketta Viro myöntää 60 miljoonaa euroa 600 bunkkerin rakentamiseen Venäjän vastaiselle 294 kilometrin pituiselle rajalleen, joihin kuhunkin mahtuu jopa kymmenen ihmistä ja jotka on suunniteltu kestämään 152 millimetrin kaliiperin ammuksen suora osuma. Baltian kehitys korostaa näiden maiden omaa sitoutumista kokonaisvaltaisen puolustuskyvyn vahvistamiseen ja yhteistyöhön alueellisen turvallisuuden varmistamiseksi. ECDI (Estonian Center for Defense Investments) allekirjoitti hiljattain noin 200 miljoonan euron arvoisen sopimuksen sekä 4x4- että 6x6-ajoneuvojen tilaamisesta Turkista, jotka se toimittaa kahdelle jalkaväkiprikaatilleen. Ensimmäisten turkkilaisten vaunujen on määrä saapua Viroon vuoden lopulla ja kaikkien muiden vuoden 2025 aikana. Joten palatakseni kysymykseen, voisiko täysimittainen sota syttyä Itämeren alueella?

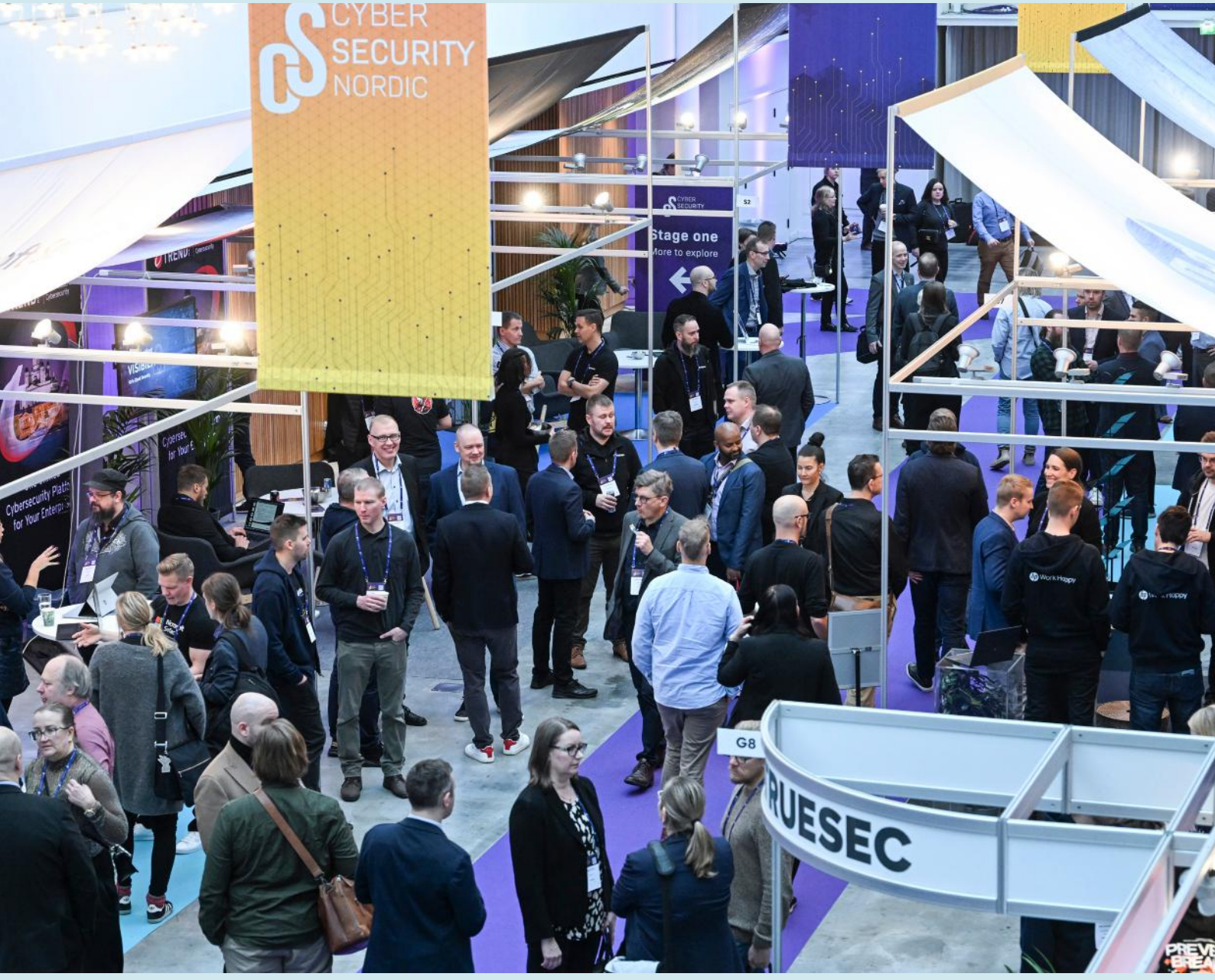
Tärkeämpää kuin sen todennäköisyyden huomioon ottaminen onko Venäjä iskemässä Baltiaan nyt, huomenna vai koskaan on kuitenkin ymmärtää, että on aika kiinnittää enemmän huomiota Euroopan puolustusteollisuuden vahvistamiseen ja keskinäiseen yhteistyöhön ja olemassaolevien resurssien yhteensovittamiseen. On myös tärkeätä ymmärtää se että voimapolitiikka on tullut jäädäkseen Eurooppaan, Ukrainaan ei ole tulossa rauhaa, entistä normaalitilaa Venäjän kanssa ei ole saavutettavissa ja olemme lähempänä laajamittaista sotaa kuin sen välttämistä. Aikajänne on lyhyt, se ei ole kymmenen vuotta vaan vuosi tai pari. Olemmeko valmiita vai edelleen mukavuusalueella? ■

DR. TIMO HELLENBERG

› CEO
Hellenberg International

CYBER SECURITY NORDIC JÄRJESTETÄÄN TÄNÄ VUONNA LOKAKUUN LOPUSSA

// Anu-Eveliina Mattila



Kaksipäiväinen Cyber Security Nordic (CSN) järjestetään tänä vuonna 29-30.10. Helsingin Messukeskuksessa ja kokoaa paikalle jälleen kansainvälisiä huippupuhujia. Tapahtuman myynti käy vilkkaana ja ohjelman suunnittelu on käynnistynyt. Tapahtuman pitchauskilpailun ilmoittautuminen avataan maaliskuun aikana.

Kuudennetta kertaa järjestettävässä tapahtumassa nousevat keskiöön kyberalan viimeisimmät trendit, innovaatiot, palvelut ja teknologiat sekä nähdään monia ensimmäistä kertaa Suomessa esiintyviä kyberalan kansainvälisiä puhujia ja huippuosaajia.

Cyber Security Nordic tarjoaa tuoreinta tietoa ja trendejä, asiantuntijoiden kohtaamisia, oivalluksia, verkostoitumista ja liiketoimintamahdollisuuksia. Tapahtuma on suunnattu kyberturvallisuuden ammattilaisille, organisaatio- ja yritysjohdolle sekä tietoturvasta ja IT:stä vastaaville asiantuntijoille.

Cyber Security Nordicin liiketoimintapäälliköksi on nimitetty Helsingin Messukeskuksessa aikaisemmin teknologian alan tapahtumien myyntipäällikkönä toiminut Anssi Rajala, Marcus Bergströmin siirryttyä Helsingin Messukeskuksen tapahtuma- ja kongressiliiketoiminnan johtajaksi.

"Cyber Security Nordic on näillä leveysasteilla ainutlaatuinen huipputapahtuma ja haluamme aikaisempaa enemmän korostaa tapahtuman suunnittelussa sitä, että kaikenkokoisten yritysten ja organisaatioiden on mahdollista saada täältä neuvoja oman digitaalisen toimintaympäristön turvaamiseen, liiketoimintariskien vähentämiseen ja aineettoman omaisuuden suojaamiseen, päivittää tietoisuuttaan ja löytää yhteistyökumppaneita näiden haasteiden haltuunottoon", sanoo Anssi Rajala.

Kaksipäiväisen tapahtuman ohjelman suunnitellaan tiiviisti alan toimijoiden ja strategisista kumppaneista muodostettavassa ohjelmaryhmässä. Ajankohtaisiin teemoihin pureudutaan niin yritysten kuin julkishallinnon näkökulmista. Keskusteluissa tulevat esille mm. Euroopan turvallinen digitalisaatio ja tietoturva, kyberrikollisuus ja lainvalvonta, demokratia, kybersota ja -puolustus sekä geopolitiikka ja kyberdiplomatia. Tapahtuman ohjelmassa käsitellään myös uusimpia ratkaisuja, jotka tukevat oppimista ja osaamisen kehittämistä. Seuraamalla Cyber Security Nordicin LinkedIniä, saat tietoa tapahtuman ohjelman kehittymisestä sekä yhteistyökumppaneista.

> **Cyber Security Nordic tarjoaa tuoreinta tietoa ja trendejä, asiantuntijoiden kohtaamisia, oivalluksia, verkostoitumista ja liiketoimintamahdollisuuksia.**

CYBER SECURITY NORDIC COMPETITION AVATAAN MAALISKUUSSA

Syksyllä valitaan jälleen kilpailun finalistit, jotka pääsevät pitchaamaan tapahtumassa 10 000 euron palkinnosta. Finalistit esittelevät tuotteensa tai palvelunsa pitchauskilpailussa Cyber Security Nordici -tapahtumassa, minkä jälkeen ammattilaisraati valitsee voittajan. Voittaja saa 10 000 euron palkinnon, jonka lahjoittaa Suomen Messusäätiö. Kilpailu oli avoin Suomessa toimiville ja rekisteröityneille kyberturvallisuusyrityksille, -tiimeille tai -organisaatioille, joiden tuote tai palvelu täyttää yhden tai useamman kilpailun kriteerin.

Cyber Security Nordic –tapahtuman järjestää Helsingin Messukeskus yhteistyössä Suomen kyberturvallisuusteollisuuden järjestön, Kyberala ry:n (FISC) kanssa. Tapahtuman strategiset kumppanien odotetaan vahvistuvan kevään aikana, jolloin he ehtivät vielä vaikuttamaan tapahtuman suunnitteluun.

Cyber Security Nordic 2023 -tapahtumassa oli ennätykselliset 47 näytteilleasettajaa, ja siihen osallistui yli 1900 yksityisen ja julkisen sektorin kyberturvallisuusammattilaista. Kansainväliset ja kotimaiset huippuosaajat pitivät ajankohtaisia esityksiä kahdella eri lavalla.

Strategisia kumppaneita olivat Accenture, HP, HSLSoftware, Huawei, Microsoft, Net Nordic, Nixu ja Trend Micro. ■

ANU-EVELIINA MATTILA

Anu-Eveliina Mattila työskentelee Helsingin Messukeskuksessa ja vastaa Cyber Security Nordic -tapahtuman viestinnästä.

KYBERALAN SOVELTAMISOPAS TUKEE YRITYKSIÄ NIS2-DIREKTIIVIN NOUDATTAMISESSA

// Peter Sund ja Risto Rajala

Euroopan Unionin NIS2-direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi hyväksyttiin vuonna 2022 ja se korvasi aikaisemman NIS1-direktiivin. Direktiivin saattaminen osaksi Suomen lainsäädäntöä on parhaillaan käynnissä ja valtioneuvosto valmistelee hetkellä esitystä laiksi kyberturvallisuuden riskien hallinnasta. Esitys on tarkoitus käsitellä eduskunnassa kevään aikana ja uuden lain soveltaminen alkaa jo 18.10.2024.

NIS2-direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta kriittisiksi katsottujen sektoreiden ja toimijoiden osalta. Tämä toteutetaan asettamalla lain soveltamisalaan kuuluville toimijoille velvoittavia riskienhallintatoimia kyberturvallisuushäiriöiden varalta. Pahantahtoisten, laittomin keinoin toimivien yksilöiden ja ryhmien aiheuttama riski verkko ja tietojärjestelmien toiminnalle, että niissä säilytettäville tiedoille on edelleen kasvamassa. Kansainvälisiin sääntöihin nojautuvat ulko-, turvallisuus- sekä kriminaalipoliittiset toimet eivät toistaiseksi ole kyenneet muuttamaan riittävästi jo pitkään jatkunutta huolestuttavaa kehityssuuntaa. Tästä syystä on edelleen perusteltua kohdistaa toimia pahantahtoisilta toimilta suojautumiseen. Yhteiskunnan toiminnan kannalta niin julkinen sektori kuin keskeisten yksityisen sektorin toimijoiden digitaalisten riskien hallintatoimet ovatkin direktiivin keskiössä. On tärkeää huomata, että Suomessa suurin osa digitaalisesta infrastruktuurista, tietojärjestelmistä sekä tiedosta on yritysten hallussa.

NIS2-direktiivin vaatimukset vaikuttavat Suomessa toimivien organisaatioiden liiketoiminnan johtamiseen, teknologia- ja kumppanivalintoihin sekä operatiiviseen valvontaan. Yritysten tulee muun muassa tunnistaa ja

arvioida säännöllisesti viestintäverkkojensa ja tietojärjestelmiensä kyberturvallisuusriskejä, toteuttaa riskienhallintatoimet, pidettävä yllä poikkeamien hallintasuunnitelmaa ja raportoitava kyberhäiriöistä määräajassa ja -muotoisesti. Yrityksen toimiva johto vastaa kyberturvallisuuden toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Tämä tarkoittaa, että toimivan johdon yleinen vastuu ulottuu säädöksen myötä myös erikseen määritetylle kyberturvallisuuden tehtäväalueelle.

Kyberturvallisuuden riskienhallintalaki määrittää sen piiriin kuuluvat toimialat, joihin kuuluvat organisaatiot jaetaan keskeisiin ja tärkeisiin toimijoihin toimialan yhteiskuntakriittisyyden ja toimijan koon mukaan. Sekä keskeisiin että tärkeisiin toimijoihin kohdistuvat käytännössä samat vaatimukset, mutta keskeisiin toimijoihin kohdistetaan etukäteisvalvontaa. Myös sanktiot ovat keskeisille toimijoille kovemmat.

NIS2-direktiivin asettamat velvoitteet digitaalisten riskien hallinnan vahvistamiseksi turvaavat yritysten liiketoiminnan jatkuvuutta, jolla voidaan ajatella olevan positiivisia vaikutuksia kannattavuuteen erityisesti pitkällä aikavälillä. Direktiivin vaatimusten täyttämisestä aiheutuu yrityksille myös suoria kustannuksia, mutta kustannukset tukevat tällöin toimitusvarmuutta ja ovat luonteeltaan ennustettavia, toisin kuin puutteellisesta digitaalisten riskien hallinnasta johtuvissa ongelma- ja epäjatkuvuustilanteissa. Riskien toteutuminen aiheuttaa tyypillisesti ennustamattomia, sekä suoria että epäasuoria kustannuksia, joiden yhteydessä voi syntyä myös vahingonkorvausvelvollisuuksia sekä pahimmillaan jo aiemmin mainittuja hallinnollisia sakkoja. Ylittämällä direktiivin edellyttämät vähimmäisvaatimukset yritys voi myös saavuttaa kilpailuetua. Yritykset hyötyvät myös laajemmin yhteiskunnan kyberkestävyyden vahvistumisesta ja luotettavammasta ja ennakoivammasta toimintaympäristöstä, joihin direktiivi vaikuttaa myönteisesti.

Kyberala ry. on jäsenistönsä kanssa laatinut NIS2-soveltamisoppaan helpottamaan yrityksiä johtamaan kokonaisturvallisuuttaan ja auttamaan lainsäädännön velvoitteiden täyttämisessä.

Suomeen sijoittautunutta kyberturvallisuusteollisuutta edustavan yhdistyksen jäsenten yhteinen, koko toimialan laajuinen projekti NIS2-direktiivin soveltamisoppaan laatimiseksi käynnistyi ydinryhmän muodostamisella syksyllä 2023. Oppaan laatimisessa on ollut mukana kymmeniä yrityksiä monipuolisesti kyberturvallisuusalan eri segmenteiltä. Kyberala on seurannut aktiivisesti NIS2-direktiivin käsittelyä ja vaikuttanut sen sisältöön. Yhdistys kannattaa vahvasti direktiivin tavoitteita ja on sitoutunut tekemään oman osuutensa sen onnistuneen toimeenpanon varmistamiseksi.

Uusien velvoitteiden tulkitseminen ja noudattaminen voi osoittautua haasteelliseksi monille direktiivin soveltamisalaan kuuluville yrityksille. Soveltamisopas valjastaa kotimaisten kyberturvallisuusalan asiantuntijoiden osaamisen ja kokemuksen apua kaipaavien yritysten tueksi. Soveltamisopas avaa uusien velvoitteiden sisältöä selkokielisesti ja havainnollistaa käytännön esimerkein digitaalisten riskien hallinnan sekä liiketoiminnan jatkuvuuden turvaamisen merkitystä. Oppaassa kuvataan, miten kansallisella lailla asetetut NIS2- direktiivin vähimmäisvaatimukset toteutetaan, hyödyntäen kolmen laajalti tunnistetun tietoturvan hallintakehikkojen soveltuvimpia osa-alueita. Tarkoituksena on havainnollistaa perustelut direktiivin vaatimuksille, kuvata tavoiteltava kyberturvallisuuden riskienhallinnan taso ja auttaa yrityksiä saavuttamaan myös konkreettisesti aiempaa matalampi riskitaso lain vaatimuksenmukaisuuden rinnalla.

Soveltamisoppaasta julkaistaan alustava versio keväällä 2024 ja opasta täydennetään, kun laki kyberturvallisuuden riskienhallinasta on lopullisessa muodossaan hyväksytty Eduskunnassa. Suomalainen kyberturvallisuusteollisuus on valmis tukemaan lain soveltamisalaan kuuluvia yrityksiä uusien velvoitteiden noudattamisessa. ■

PETER SUND

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

RISTO RAJALA

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

POIMINNAT CYBERWATCHFINLAND VIIKKOKATSAUKSISTA

// Cyberwatchin analyysitiimi

TÄSSÄ KOOSTEESSA SEURAAVAT ARTIKKELIT

VIIKOLTA 5:

- Syväväärennökset ja Kiina uhka huolestuttavat Yhdysvalloissa

VIIKOLTA 6:

- Palvelunestohyökkäysten tylsyvä kärki

VIIKOLTA 8:

- Ukraina voitti informaatiosodan – onko sillä väliä?

VIIKOLTA 9:

- Alustajätit taistelevat disinformaatiota vastaan EU:ssa, myös digipalvelusäädös velvoittaa

SYVÄVÄÄRENNÖKSET JA KIINA UHKA HUOLESTUTTAVAT YHDYSVALLOISSA

Yhdysvaltain turvallisuusviranomaiset ovat huolissaan ulkopuolisesta sekaantumisesta syksyllä edessä oleviin presidentinvaaleihin. Aiheesta varoittivat tammikuussa sekä kansallinen turvallisuusvirasto NSA että liittovaltion poliisi FBI. Huolet liittyvät erityisesti tekoälypohjaisiin syvävääreennöksiin (engl. deepfake), joiden uskottavuus kehittyy jatkuvasti. Jos edellisissä presidentinvaaleissa eniten epäselvyyttä aiheutti äänten laskun epäselvyydet ja vaalituloksen kiistäminen, näissä vaaleissa suurin uhka viranomaisten mukaan on yleinen kaaos, jonka väärennökset voisivat aiheuttaa.

Syvävääreennöksellä tarkoitetaan aidolta vaikuttavaa kuvaa tai ääntä sisältävää väärennöstä, joka on tuotettu koneoppivan tekoälyn avulla. Nämä ovat varsin suosittuja, ja esimerkiksi TikTokista ja YouTubesta löytyy useita suosittuja videoita, joissa poliitikot tai julkisuuden henkilöt on laitettu keskustelemaan keskenään mitä erinäisimmistä aiheista, kuten vaikkapa videopeleistä. Vaalien kontekstissa syvävääreennökset toimivat keinona levittää väärää tietoa sekä vaikuttaa vaalitulokseen. Ennakkomerkkejä niiden muodostamasta uhkasta Yhdysvalloissa nähtiin tammikuussa, kun demokraattien esivaalien aikaan työkaluna käytettiin väärennöspuheluita, joissa ääni oli muutettu istuvan presidentti Joe Bidenin ääneksi. Tämän avulla suoritettiin puhelukampanja New Hampshiren osavaltiossa, joissa ihmisiä kehotettiin jättämään äänestämättä. Häirinnän vaikuttavuus jäi epäselväksi, mutta vastaavanlaiset kampanjat lähempänä varsinaisia vaaleja ja esimerkiksi sosiaalisessa mediassa leviävinä voisivat pahimmillaan vaikuttaa äänestyskäyttäytymiseenkin.

Yhdysvalloissa syvävääreennökset ovat herättäneet huolen myös ulkomaiden mahdollisesta sekaantumisesta vaaleihin. Erityisesti viranomaisten puheenvuoroissa on korostunut huoli Kiinasta ja sen valtavista kyberresursseista. Vaikka Kiinaa ei puheenvuoroissa suoraan syytetty syvävääreennösten tekemisistä, huomioitiin sen olevan tekoälyn suurvalta ja Yhdysvaltain merkittävin kilpailija myös tämän teknologian saralla. Kiinalaista kybervaikuttamista on nähty vastikään Taiwanin presidentinvaaleissa yhteydessä muun muassa suurena määränä kyberhyökkäyksiä sekä valeuutisia, joten uhka tulee ottaa vakavasti. Pelkästään Kiinaan keskittyminen jättäisi kuitenkin auki useita muita toimijoita. Tapahtumat vuoden 2016 vaalien aikaan on varmasti edelleen muistissa. Niistä tehdyn selvityksen, niin kutsutun Muellerin raportin mukaan, venäläiset turvallisuuspalvelut pyrkivät aktiivisesti edistämään Donald Trumpin valintaa presidentiksi muun muassa sosiaalisessa mediassa vaikuttamalla, eri kohteita hakkeroimalla ja julkaisemalla erinäisiä dokumentteja.

Syvävääreennökset eivät ole vain amerikkalaisten haaste. Marraskuussa Slovakiassa äärioikeistolainen Republika-puolue käytti liberaalin edistyspuolueen johtajan ääntä syvävääreennöksessä osana vaalikampanjaansa. Vaalikampanjan aikaan esitettiin myös toisesta saman puolueen edustajasta tasokas väärennös, jossa ikään kuin salassa äänitetyssä keskustelussa puhuttiin äänten ostamisesta. Slovakiassa on käytössä niin sanottu vaalirauha, mikä tarkoittaa sitä, että vaaleista uutisointi tulee lopettaa tietyn aikaa ennen äänestystä. Tämän vuoksi faktantarkistuskin jäi näissä tapauksissa tavallisten kansalaisten ja sosiaalisen median käsiin.

Taistelussa väärää tietoa vastaan avainasemassa ovat faktojen tarkastus, lähdekritiikki ja hyvä medianlukutaito. Jos näissä on puutteita ja erityisesti jos media ja yhteiskunnallinen keskustelu ovat Yhdysvaltojen tapaan polarisoituneita, myös väärennökset voivat upota hedelmällisempään maaperään.

PALVELUNESTOHYÖKKÄYSTEN TYLSYVÄ KÄRKI

Helmikuun ensimmäisinä päivinä Suomessa saatiin jälleen kokea uusi palvelunestohyökkäysten aalto, jonka takana oli jo aiemmin tutuksi tullut venäläinen NoName057(16)-ryhmittymä. Kyseinen itsensä patrioottiseksi venäläiseksi haktivistiryhmäksi mieltävä toimija toteuttaa jatkuvasti palvelunestohyökkäyksiä kohteisiin ympäri maailmaa. Usein ne pyritään ajoittamaan kansallisesti merkittäviin päiviin tai hetkiin, jolloin hetkelliset palvelukatkokset saisivat mahdollisimman paljon huomiota. Suomessa iskut ajoittuivat samoille päiville kuin monien alojen lakot ja hallituksen politiikkaa vastustavat mielenosoitukset. Myös hakkeriryhmä itse ilmoitti iskujen syyksi ”Suomen kansan tukemisen Ukrainan rikolliselle hallitukselle rahaa syytävän ja omat kansalaiset hylkäävän hallituksen toimia vastaan”. Iskut kestivät parin päivän ajan, kunnes ryhmä tapojensa mukaisesti siirtyi seuraavan maan kimppuun. Kolmas helmikuuta ryhmän Telegram-kanava olikin jo täynnä postauksia Ranskan rikollisesta tuesta Ukrainalle ja kuinka maan viranomaiset ja yritykset tulevat vapisemaan palvelunestohyökkäystenaallon alla.

Palvelunestohyökkäyksissä ei ole mitään uutta, ja NoNamen operaatiot tuntuvat Suomessakin menettäneen vaikuttavuuttaan. Hyökkäysten tavoite on ensisijaisesti huomion herättäminen ja kansallisen epävarmuuden lisääminen, mutta vaikuttaa siltä, että palvelunestohyökkäyksiin on jo totuttu ja ne ymmärretään matalan tason häirinnäksi verrattuna vaarallisiin kyberhyökkäyksiin. Media toki tarttui hyökkäysaaltoon, mutta uutisointi ei ollut sensaatiohakuista, vaan tyylinä vaikutti enemmänkin olevan tiedon välittäminen siitä, mitä on meneillään, ja mitä palvelunestohyökkäykset tarkoittavat. Tämä on paitsi luonnollista, myös tärkeää. Median on pakko nostaa esiin varsinkin näin laaja hyökkäysaalto, jonka vaikutuksena useiden kaupunkien ja merkittävien yritysten verkkosivut kokevat samanaikaisesti häiriöitä. Palvelunestohyökkäyksistä, etenkin koordinoiduista hyökkäysaalloista tulee pitää kansa tietoisena, vaikka todelliset vaikutukset iskujen kohdalla ovatkin sekä lyhytkestoisia että vähäisiä. Mikäli tätä ei tapahtuisi voisi hyökkääjien tavoite onnistua huomattavasti paremmin, kun kansalaiset huomaisivat arkipäivässä käytettävät palvelut toimimattomiksi ilman tietoa siitä, mistä todellisuudessa on kyse. Vaikuttaakin siltä, että Suomen kansallinen resilienssi on tämän uhkan osalta kasvanut eikä palvelunestohyökkäyksillä saavuteta sitä vaikutusta, mihin uhkatoimija niillä näyttää pyrkivän.

On kuitenkin huomioitava, että palvelunestohyökkäyksien arvo informaatiovaikuttamisen työkaluna ei ole pelkästään kohdevaltion kansalaisiin kohdistuva. Etenkin julkisesti operaatioistaan ilmoittavan ryhmän, kuten juuri NoName057:n kohdalla oleellista on myös viestintä

ryhmää ja sen aatetta tukeville ja sen sosiaalisen median kanavien seuraajille. Näille kanaville postataan kuvia hetkellisesti alhaalla olevista sivuista ja kuvaillaan vuolaasti, miten kohdemaan kansalaisten elämä vaikeutuu huomattavasti heidän toimiensa vuoksi. Tämän avulla saadaan ylläpidettyä kuvaa siitä, että länsimaat kärsivät jatkuvasti venäläisistä kyberhyökkäyksistä, ja mahdollisesti saadaan jopa rohkaistua uusia hakkereita liittymään isänmaalliseen kyberrintamaan. NoName057:n Telegram-kanavalla postataankin paljon myös lähes valheellisia ilmoituksia hyökkäyksistä, jotka todellisuudessa eivät vaikuttaneet merkittävästi kohdepalvelun saatavuuteen tai joita ei kohdemaassa edes huomattu. Esimerkiksi pelkästään tammikuun viimeisellä viikolla samainen ryhmä oli ilmoittanut tehneensä Suomeen hyökkäyksiä kolmessa eri erässä ja kohteina oli väitetysti esimerkiksi kyberturvallisuuskeskus, oikeusministeriö ja Helsingin kauppakamari, mutta nämä tapahtumat eivät Suomessa edes ylittäneet uutiskynnystä. Kyseessä saattoi toki olla vähemmällä intensiteetillä toteutetut operaatiot. Tästä voi kertoa myös se, että niitä ei ollut edes pyritty ajoittamaan yhteiskunnallisesti merkittäviin hetkiin. Ryhmä ilmoitti silti niistä kanavallaan samankaltaisella rehvakkuudella kuin helmikuun alkupäivien iskuista.

Palvelunestohyökkäykset eivät kuitenkaan ole täysin harmittomia. Niillä voidaan myös aiheuttaa todellista harmia, mikäli ne onnistutaan ajoittamaan hetkiin, jolloin tiedonsaanti kohteena olevista palveluista olisi erittäin kriittistä. Esimerkiksi kriisien tai muiden poikkeuksellisten tapahtumien kohdalle ajoitetut palvelunestohyökkäykset saattavat toimia tehokkaasti epävarmuuden edistäjinä, vaikka tiedettäisiinkin täysin mistä niissä on kyse. Vaikka yleisesti ne eivät muodostakaan merkittävää uhkaa, ei tule tuudittautua näennäiseen turvallisuuden tunteeseen tai ajatukseen siitä, että vaikuttamiselta ollaan täysin suojassa. Hyökkäykset tuleekin ymmärtää monella eri tavalla informaatiovaikuttamisen tavoitteita palvelevana työkaluna. Ne tuskin tulevat katoamaan Suomen tai länsimaiden kyberympäristöstä ja siksi niihin tulee sekä tottua että varautua. Positiivista on, että hyökkäysten vaikuttavuus vähenee kuitenkin jatkuvasti, kun organisaatiot kehittävät kykyään ylläpitää toimintoja iskun kohteeksi joutuessaan, ja kansalaiset tiedostavat paremmin mistä hyökkäyksissä on kyse.

UKRAINA VOITTI INFORMAATIOSODAN – ONKO SILLÄ VÄLIÄ

Informaatiosodankäynti on keskeinen osa jokaista modernia konfliktia, myös Ukrainan sotaa. Informaatiovaikuttamisen keinoilla pyritään vaikuttamaan käynnissä olevan konfliktin lopputulokseen. Informaatiovaikuttamisella tarkoitetaan toimintaa, jolla pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin. Tavoitteita ovat muun muassa oman agendan tukeminen tai vaihtoehtoisesti epäluottamuksen lietsominen kohdeyhteiskunnassa. Edelleen informaatiovaikuttamista voi tapahtua yksittäisinä tekoina tai laajoina vaikuttamiskampanjoina esimerkiksi bottiverkkojen, sosiaalisen median tai muiden viestinnällisten keinojen avulla. Tämä voi näkyä muun muassa väärien tai harhaanjohtavien tietojen levittämisenä sekä sinänsä oikean tiedon tarkoitushakuisessa käytössä.

Ukrainan voidaan ajatella voittaneen Venäjän informaatiosodankäynnissä ainakin länsimaissa. Tästä esimerkkinä ovat Ukrainan esittämien narratiivien ja käsitysten dominointi, joiden voidaan nähdä vieneen voiton venäläisten esittämästä vaihtoehtoisesta tapahtumankulusta. Etenkin sodan alkuvaiheessa Ukrainan strateginen viestintä oli erityisen onnistunutta. Sotaan liittyvät tarinat ja meemit levisivät ympäri maailman. Vastaavasti Venäjä on epäonnistunut oman narratiivinsa levittämisessä. Ennen sotaa Venäjän informaatioasetta ja trolleja pelättiin paljon, mutta niiden vaikuttavuus sekä Ukrainassa että länsimaissa on jäänyt vähäiseksi. Vaikka ristiriitoja suhtautumisessa Ukrainaan ja ukrainalaisiin pakolaisiin on esiintynyt, on Eurooppa jopa hämmentävän yhtenäisesti seissyt maan tukena. Tässä merkittävä rooli on Ukrainan onnistuneella viestinnällä sekä länsimaisella medialla, joka on asettunut selkeästi tukemaan Ukrainaa sodassa. Venäjän informaatiovaikuttamisessa on toki muistettava, että sen ei välttämättä ole tarkoituskaan vakuuttaa länsimaita, vaan kohderyhmänä ovat maan omat kansalaiset sekä Euroopan ulkopuoliset maat.

Toisaalta on viitteitä siitä, että Venäjä hallitsee oma informaatiotilaansa suhteellisen hyvin eivätkä Ukraina tai länsimaat pysty myöskään vaikuttamaan Venäjän kansalaisiin. Suurta sodan vastaista liikehdintää maassa ei ole tapahtunut Venäjän kansalaisille suunnatusta tiedottamisesta huolimatta, vaikka taustalla toki vaikuttaa autoritäärisen yhteiskunnan luonne ja protestoinnista seuraavat sanktiot. Venäläisestä informaatiotilasta kertoo kuitenkin myös tutkimuskeskus Levadan tilastot siitä, että sodan aikana Putinin tuen määrä on kasvanut samalla, kun asenteet länsimaihin heikentyneet. Vaikka Venäjältä tuleviin tilastoihin tulee aina suhtautua varauksella, on Levadaa perinteisesti pidetty yhtenä luotettavammista informaation lähteinä maassa. Venäjän kotimaahan suunnattu informaatiovaikuttaminen näyttäytyykin tässä valossa tehokkaalta. Toisaalta riippumatonta tietoa haluaville tietoa varmasti olisi saatavilla esimerkiksi itsenäisiltä Telegram-kanavilta ja usein ulkomailta toimivilta oppositiomedioilta. On kuitenkin huomattava kynnys hankkia tietoa avoimesti omaa hallintoa vastustavilta lähteiltä, ja venäläisten on äärimmäisen helppoa myös yksinkertaisesti ummistaa silmänsä sodalta. Ukrainan on käytännössä mahdotonta tunkeutua tämän informaatiomuurin sisäpuolelle, ja onkin epätodennäköistä, että Venäjä menettäisi hallinnan omien rajojensa sisäpuolella vallitsevista narratiiveista.

Informaatiosotaa käydään jatkuvasti. Vaikka Ukraina on jo voittanut länsimaiset sydämet puolelleen, käy maa myös informaatioympäristössä eräänlaista kulutussotaa. Viime aikoina lännenkin mediassa esille on noussut aiempaa enemmän uutisia Ukrainan haasteista, kuten miehistö- ja ammuspulasta. Myös Ukrainan tappion mahdollisuutta ja tarvetta rauhalle on väläytelty. Ukrainan haasteena on ylläpitää ihmisten mielessä omia narratiiveja ja sotaa edelleen ajankohtaisena, tärkeänä ja kansainvälisenä. Kotimaassa kriittistä on ylläpitää omien kansalaisten moraalia, uskoa voittoon ja tukea sotatoimien jatkamiselle. Loppujen lopuksi avainkysymykseksi nousee, kuinka Ukraina onnistuu muuttamaan informaatioherruuden konkreettiseksi kotimaiseksi ja länsimaiseksi tueksi. Informaatiosodan voitto ei lämmitä, mikäli taistelukentällä tarjolla on vain hopeamitali.

ALUSTAJÄTIT TAISTELEVAT DISINFORMAATIOTA VASTAAN EU:SSA, MYÖS DIGIPALVELUSÄÄDÖS VELVOITTAA

Disinformaation vastainen rintama Euroopassa sai uusia vahvistuksia helmikuussa, kun Google ja Meta ilmoittivat tahoillansa aloittavansa kampanjat disinformaation torjumiseksi kesäkuisten europarlamenttivaalien kontekstissa. EU:ssa on pelätty erityisesti Venäjän propagandan määrän kasvua ja vaikutuksia tuleviin vaaleihin. Yhtiöiden ilmoitukset ajoittuivat symbolisesti sopivasti Euroopan unionin digipalvelusäädöksen DSA (Digital Services Act) kansallisten soveltamisen alkamisen, helmikuun 17. päivän, läheisyyteen. DSA:n on toivottu omalta osaltaan torjuvan disinformaatiota, sillä se asettaa verkkoalustoille velvoitteita muun muassa alustojen moderoinnin suhteen sekä velvoittaa alustoja arvioimaan ja vähentämään demokraattisiin- ja vaaliprosesseihin liittyviä riskejä. DSA:n velvoitteita on sovellettu erittäin suurten verkkoalustojen ja hakukoneiden osalta jo viime elokuun 25. päivästä alkaen.

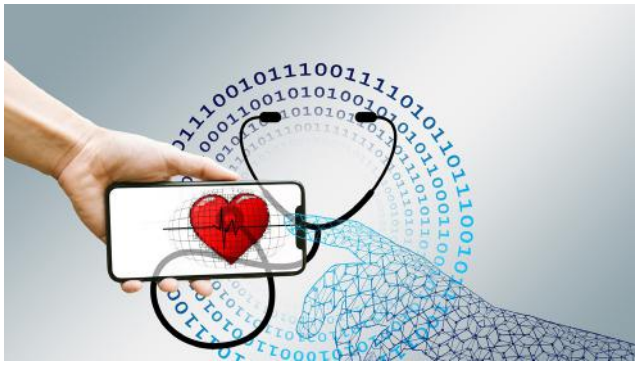
Googlen tapauksessa yhtiö aloittaa huhti-toukokuussa mainoskampanjan, joka toteutetaan muun muassa YouTube- ja TikTok-alustoilla viidessä eri EU-maassa: Belgiassa, Ranskassa, Saksassa, Italiassa ja Puolassa. Mainokset sisältävät tietoa siitä, miten tunnistaa mis- ja disinformaatio ja minkälaista väärää tietoa pyritään levittämään. Kampanjassa hyödynnetään niin kutsuttua ”prebunking”-tekniikkaa. Tämä tarkoittaa sitä, että ilmoitus väärästä tiedosta pyritään saamaan kohteelle aiemmin kuin itse väärä tieto tavoittaa kohteen. Näin väärän tiedon saavuttaessa kohteen, osaa hän jo suhtautua siihen varauksella. Kyseisten maiden valitsemista mainosten kohteeksi perusteltiin muun muassa mahdollisuutena tavoittaa laaja määrä vaalien äänestäjiä sekä hyödyntää yhtiön omaa paikallistietoutta. Vaikka kampanjan kohteena ovat EU:n väkirikkaimmat valtiot, jää sen ulkopuolelle kuitenkin merkittävä määrä muiden jäsenmaiden äänestyskelpoisia kansalaisia, mikä osaltaan heikentää vaikuttavuutta. Toimet ovat kuitenkin eittämättä paikallaan ja oikeansuuntaisia.

Meta taas tarttuu ongelmaan avaamalla erityisen vaalikeskuksen (Elections Operation Center), joka pyrkii tunnistamaan ja torjumaan uhkia reaaliaikaisesti. Misinformaatiota torjutaan muun muassa yhteistyössä 26 kumppanin kanssa ympäri EU:ta yli 22:lla eri kielellä faktantarkastuksen avulla. Lisäksi pyrkimyksenä on taklata koordinoidut vaikuttamisoperaatiot sekä vastata tekoälyllä toteutettaviin mahdollisiin väärinkäytöksiin kuten syvävääreennöksiin.

Molempien yhtiöiden päätösten taustalla vaikuttaa varmasti osittain EU:n digipalvelusäädös, vaikka ilmoituksissa ei suoraan siihen viitatakaan. Säädöksen päätavoitteena EU-komission mukaan on ”estää laitonta ja haitallista toimintaa verkossa ja torjua disinformaation leviämistä.” Digipalvelusäädös on julkisuudessa saanut tähän asti kuitenkin enemmän huomiota muun muassa sen myötä tulleesta velvollisuudesta antaa alustojen käyttäjille mahdollisuus kieltää personoitu markkinointi, velvoitteesta luoda helposti ymmärrettävät käyttöehdot sekä velvoitteesta avoimempaan sisällön moderointiin ja mahdollisuuteen valittaa moderointipäätöksestä. Lisäksi DSA kieltää yksiselitteisesti mainonnan kohdentamisen lapsille sekä mainonnan kohdistamisen aikuisille esimerkiksi etnisen taustan tai seksuaalisen suuntautumisen perusteella. Tavoitteena on siis kasvattaa käyttäjien oikeuksia ja vaikutusmahdollisuuksia.

Vaikka säädös itsessään koskee käytännössä kaikkia digitaalisia palveluita, sen keskiössä ovat erittäin suuret verkkoalustat ja hakukoneet. Tällaisiksi määritelmällisesti luetaan palvelut, joiden aktiivisten käyttäjien määrä kuukaudessa ylittää kuuden kuukauden ajanjakson keskiarvon tarkastelussa 45 miljoonaa käyttäjää EU-alueella. Näille erittäin suurille toimijoille lisävelvollisuuksina on neljän erillisen riskikategorian arviointi, joiden osalta tulisi ryhtyä myös toimiin riskien vähentämiseksi. Näitä ovat laittoman sisällön levittämiseen, kuten esimerkiksi laittoman vihapuheen leviämiseen sekä demokraattisiin prosesseihin, kansalaiskeskusteluun ja vaaliprosesseihin liittyvät riskit. Sakkojen enimmäismäärä säädöksen velvoitteiden noudattamatta jättämisestä voi olla korkeintaan 6 % yrityksen vuotuisesta maailmanlaajuisesta liikevaihdosta.

EU-sääntelyä nimitetään usein byrokraattiseksi ja sen saavutuksia epäillään. On kuitenkin selvää, että sillä on myös positiivisia vaikutuksia. DSA onkin mahdollisesti esimerkki kansalaisen näkökulmasta onnistuneesta sääntelystä, sillä se lisää palveluiden läpinäkyvyyttä ja käyttäjien valinnanmahdollisuuksia oman yksityisyytensä suhteen. Laajemmalle yhteiskunnalle hyödyt näkyvät juuri edellä kuvattujen kampanjoiden muodossa, jotka omalta osaltaan voivat vähentää vihamielisten toimijoiden EU:hun kohdistamien vaikutusyritysten tehokkuutta. ■



LÄHTEET

SYVÄVÄÄRENNÖKSET JA KIINA UHKA HUOLESTUTTAVAT YHDYSVALLOISSA:
https://cybernews.com/news/fbi-nsa-cybersecurity-election-interference/
https://www.cnbc.com/2024/01/10/how-fbi-nsa-are-preparing-for-deepfakes-ahead-of-2024-elections.html
https://faktabaari.fi/fakta/presidenttiehdokkaiden-puheita-on-kloonattu-ja-muokattu-tekoalylla/
https://www.justice.gov/archives/sco/file/1373816/download
https://www.nbcnews.com/politics/2024-election/fake-joe-biden-robocall-tells-new-hampshire-democrats-not-vote-tuesday-rcna134984
https://www.nbcnews.com/tech/misinformation/joe-biden-new-hampshire-robocall-fake-voice-deep-ai-primary-rcna135120
https://www.politico.eu/article/china-bombards-taiwan-with-fake-news-ahead-of-election/
https://yle.fi/a/74-20056699
https://yle.fi/a/74-20071490

PALVELUNESTOHYÖKKÄYSTEN TYLSYVÄ KÄRKI:
https://t.me/s/noname05716eng
https://www.hs.fi/talous/art-2000010202403.html
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-jatkuvat-myos-vuonna-2024

UKRAINA VOITTI INFORMAATIOSODAN – ONKO SILLÄ VÄLIÄ?:
Cyberwatch Finlandin viikkokatsaus viikko 8/2024

ALUSTAJÄTIT TAISTELEVAT DISINFORMAATIOTA VASTAAN EU:SSA, MYÖS DIGIPALVELUSÄÄDÖS VELVOITTAA:
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_fi
https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops
https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms
https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32022R2065#d1e2324-1-1
https://faktabaari.fi/nakokulmat/nakokulma-digipalvelusaados-lisaa-avoimuutta-ja-vahvistaa-kayttajien-oikeuksia/
https://prebunking.withgoogle.com/
https://blog.google/around-the-globe/google-europe/supporting-elections-for-european-parliament-2024/
https://about.fb.com/news/2024/02/how-meta-is-preparing-for-the-eus-2024-parliament-elections/

KUUKAUSIKATSAUS TAMMIKUU/2024

// Cyberwatchin analyysitiimi

SISÄLLYS:

TÄSSÄ KATSAUKSESSA

Tässä kuukausikatsauksessa tarkastelemme edellisen vuoden merkittävimpiä kybermaailman ilmiötä sitoen ne laajempiin kokonaisuuksiin. Katsaus jakautuu kolmeen tarkastelukulmaan: jatkuviin seurannan kohteisiin, ilmiöihin, joita haluamme erityisesti edellisestä vuodesta korostaa sekä ilmiöihin, joiden kehitystä kannattaa seurata.

Kansainvälisen kyberympäristön osalta on syytä huomata, että se näyttäytyi edelleen vuonna 2023 vailla sääntöjä olevana, jopa anarkistisena tilana. Tästä kielivät muun muassa konfliktien leviäminen kybermaailmaan, hyökkäysten vaikutukset siviileihin sekä puuttuva kansainvälinen lainsäädäntö. Niin EU kuin YK ovat pyrkineet ulottamaan vaikutusvaltaansa kyberturvallisuuden alueelle, mutta yhteisten globaalien pelisääntöjen luomisesta ollaan edelleen kaukana.

Kyberrikollisuuden kehittyi uuden teknologian ja uusien tekomuotojen yleistyessä entistä tehokkaammaksi. Kyberrikollisuus myös kasvatti merkitystään valtioiden välisessä kanssakäymisessä, ja rajat fyysisen maailman järjestäytyneen rikollisuuden ja kyberrikosten välillä hämärtyivät entisestään.

Teknologiassa selvästi merkittävin ilmiö vuonna 2023 oli tekoälyteknologian yleistymisen luoma murros. Erilaisten tekoälysovellusten määrä ja käyttömahdollisuudet kasvoivat räjähdysmäisesti, ja niistä saatiin hyötyä niin kyberturvallisuuden edistämisessä kuin rikollisen toiminnan tehostamisessa. Teknologian kentän kehityskohteet eivät kuitenkaan rajautuneet vain tekoälyyn, vaan myös esimerkiksi kilpailu mikrosirujen tuotantokyvystä Yhdysvaltojen ja Kiinan välillä jatkui kiivaana.

Muista tämän vuoden ilmiöistä haluamme korostaa kybersodan kehitystä Ukrainan ja Venäjän välisessä konfliktissa sekä ideologisesti motivoituneiden kyberaktivistien eli haktivistien roolia. Ensi vuoden merkittävistä muutoksista korostamme NIS2-direktiivin luomia vaatimuksia sekä kasvavaa kriittiseen infrastruktuurin kohdistuvaa kyberuhkaa.

1.TAPAHTUMIA VUODEN 2023 KYBERMAISEMASSA

1.1. Kansainvälinen kyberympäristö

Vuotta 2023 voisi kuvailla kybermaailman kansainvälisen anarkian vuodeksi. Kansainvälisten suhteiden tutkimuksessa käytettävällä termillä tarkoitetaan tilannetta, jossa maailmalta puuttuu ylin auktoriteetti tai suvereniteetti, joka voisi ratkaista riitoja, valvoa lakia tai järjestää kansainvälistä järjestelmää. Vertauskuva on osuva myös kybermaailmassa. Valokeilassa ovat vuoden aikana olleet useat eri asiat: Ukrainan ja Venäjän kyberympäristössä näkyvä sota, Yhdysvaltain ja Kiinan kauppasota, esimerkiksi pakotteet mikrosiruteknologiassa, sekä vapaaehtoisten hakkerien ja haktivistiryhmien suorittamat kyberhyökkäykset eri konflikteissa. Kyberympäristö näyttäytyikin kaoottisena ja sääntöjä vailla olevana harmaana alueena.

Viime vuonna kyberhyökkäykset koskettivat entistä useammin tavallisia kansalaisia muuallakin kuin sodan keskellä olevassa Ukrainassa. Esimerkiksi Naton huippukokouksessa kesällä isäntäkaupunki Vilnan joukkoliikenteeseen kohdistui kyberiskuja, jotka vaikuttivat myös tavallisten ihmisten elämään. Tapahtuman ei myöskään tarvitse olla suoraan poliittinen: esimerkiksi Pariisin tulevien kesäolympialaisten järjestäjä Ranska on ilmoittanut olevansa huolissaan kyberhyökkäysten määrän mahdollisesta kasvusta kisojen aikana.

Ratkaisua kybermaailman anarkiaan tuskin on tulossa, vaikka yrityksiä nähtiin vuoden 2023 aikana. Etenkin EU kunnostautui viime vuonna kybermaailmaa sivuavassa säätelyssä. Tavoitteena on Bryssel-efekti, jolla tarkoitetaan ilmiötä, jossa Euroopan unionin laatima sääntely omaksutaan myös muualla maailmassa. Esimerkiksi kesällä Yhdysvaltojen kanssa hyväksytty tiedonsiirtosopimus, syksyllä yksityisyysaktivisteja huolestuttanut Chat Control –aloite, NIS2-kyberturvallisuusdirektiivi sekä työn alla oleva tekoälyregulaatio ovat merkittäviä, vaikka niiden globaalista leviämisestä ei ole takeita. Myös Yhdistyneet kansakunnat on pyrkinyt ottamaan johtajuutta: viime vuoden aikana valmisteltavana ollut kyberrikollisuussopimus näkee mahdollisesti päivänvalon vuonna 2024. Sopimuksella pyrittäisiin helpottamaan valtioiden välistä tiedonjakamista sekä muodostamaan yhteinen käsitys siitä, mitä kyberrikollisuudella tarkoitetaan. Sopimus on ollut vastatuulessa, sillä lähteiden mukaan neuvottelevat maat ovat jakautuneet blokkeihin, joissa toisella puolella ovat autoritääriset valtiot, toisella puolella länsimaat.

Valtioiden kyvyttömyys turvata kyberympäristöä tai säännellä siellä vallitsevaa anarkiaa onkin ollut silmiinpistävä. Jos EU, YK tai valtiot muissa puitteissa eivät pysty tuomaan järjestystä kybermaailmaan, yhdeksi vaihtoehdoksi nousee muiden toimijoiden esittämät aloitteet. Esimerkiksi Punaisen Ristin kansainvälinen komitea julkaisi lokakuussa kahdeksan säännön ohjelistan kyberoperaatioita suorittaville siviilihakkereille. Toistaiseksi on aikaista sanoa, kuinka hyvin sääntöjä noudatetaan, vai noudatetaanko ollenkaan, mutta kyseessä on kuitenkin avaus oikeaan suuntaan. Yleismaailmallisten kyberlakien puuttuessa mahdollinen kehityskulku on entistä rajumpi blokkiutuminen liittolaispiireihin. Uhkatiedon jakaminen ja puolustuksellinen yhteistyö on jo nyt rajoittunut selkeästi liittolaisuuksien mukaan.

1.2. Kyberrikollisuus

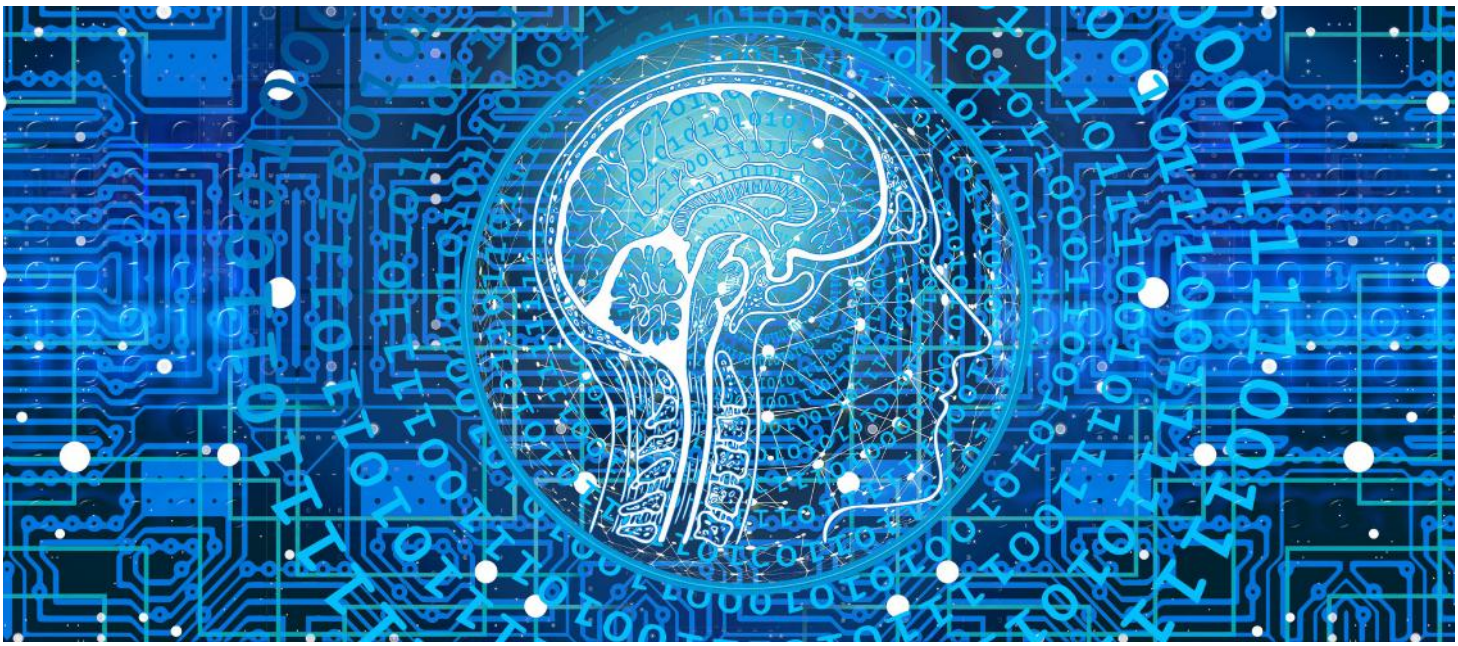
Vuonna 2023 kyberrikollisuutta parhaiten kuvaava termi on jatkuva muutos. Viime vuoden aikana tämä saatiin kokea usealla tavalla. Oli kyse sitten uuden teknologian mukaantulosta, toimintatapojen kehittymisestä tai täysin uudenlaisista rikostyypeistä, viime vuonna lähes joka viikko nousi esiin jokin uudenlainen kyberrikollisuuden piirre. Tämän ei toisaalta pitäisi tulla yllätyksenä, sillä ilmiö on käytännössä koko olemassaolonsa aikana ollut muutoksessa kehittyen aina sen mukaan, miten rikosten uhrit ja viranomaiset pystyvät olemassa oleviin toimintatapoihin vastaamaan. Merkittävät muutokset kyberrikollisuudessa eivät yleensä olekaan niinkään täysin uudenlaisia toiminnan muotoja, vaan jo olemassa olevien tekotapojen kehittymistä entistä haastavampaan ja ennakoimattomaan suuntaan. Monella tavalla rikokset sinänsä ovat jo ennestään tuttuja, mutta niiden toteuttamiseen käytettävät työkalut tai toteuttamistavat vain kehittyvät.

Hyvä esimerkki tästä on kiristyshyökkäyksien kehitys. Jo aiemmin alkanut, mutta etenkin viime vuonna korostunut trendi kiristyshyökkäyksissä oli, että uhkavaatimus kohdistuu datan palauttamisen sijaan tai lisäksi entistä useammin uhkaan datan vuotamisesta tai tietojen avoimesta julkaisemisesta. Näissä kaksois- tai kolmoiskiristyksen nimellä tunnetuissa iskumuodoissa uhrilta vaaditaan lunnaita usean eri uhkauksen avulla, ja usein myös monta kertaa. Tämänkaltainen hyökkäystapa on kehittynyt vastauksena siihen, että organisaatiot ovat useasti varautuneet kiristykseen datan varmuuskopioiden ja varajärjestelmien myötä, joten pelkällä datan palauttamisella kiristäminen on tehotonta. Toisaalta ilmiötä tukee myös kyberhyökkäyksiin liitettävä entistä suurempi mainehaitta ja organisaatioiden väliset keskinäisriippuvuudet. Jos yritys joutuu kyberhyökkäyksen kohteeksi ja varastettu data julkaistaan, voi sen olla vaikea vakuuttaa yhteistyökumppaneita siitä, ettei mitään heihin liittyvää ole vuotanut, saati ansaita uusien potentiaalisten kumppaneiden luottamusta.

Toinen esimerkki rikollisuuden kehittymisestä löytyy jo vuosia kyberrikollisuuden yhtenä tehokkaimmista ja suosituimmista toiminnanmuodoista olleesta tietojen kalastelusta. Viime vuoden aikana ei kalastelu sinänsä muuttunut mitenkään, sillä sen tavoitteet ja periaatteet pysyivät täysin samana, mutta uuden teknologia, etenkin tekoälyn, ja uudenlaisten kohteiden ja keinojen avulla toiminta muuttui entistä tehokkaammaksi ja vaikeammin havaittavaksi. Kalasteluviestit kehittyivät, uhreihin kohdistettiin uusilla tavoin painetta ja operaatiot laajenivat, kun viestien jakelu ja usealle kielelle kääntäminen tulivat entistä uskottavimmiksi, helpommiksi ja halvemmiksi.

Vuonna 2023 kyberrikollisuus muuttui pääasiallisesti olemassa olevien toiminnan muotojen kehittymisen myötä. Samalla toiminta kuitenkin muuttui entistä organisoidumpaan ja järjestäytynempään suuntaan. Rajat kyberympäristössä toteuttavan rikollisuuden sekä fyysisen maailman järjestäytyneen rikollisuuden, tai valtiollisten operaatioiden välillä hämärtyivät entisestään. Kyberrikollisuus on äärimmäisen tuottavaa, ja sen merkitys kasvaa vuosi vuodelta. Onkin hyvin todennäköistä, että myös vuonna 2024 tullaan näkemään kehitystä jo olemassa olevien kyberrikosten toteuttamisessa, ja varmasti monta yllätystä, kun rikolliset keksivät jälleen uusia tapoja ihmisten huijaamisessa tai teknisten suojausjärjestelmien kiertämisessä.

Lähteet sivulla 41



1.3. Teknologia

Vuodesta 2023 ei voida teknologian kehityksen suhteen puhua mainitsematta tekoälyn räjähdysmäisen suosion ja käyttömahdollisuuksien kasvua. Kyseessä ei ole pelkästään viime vuoden, vaan mahdollisesti jopa kuluvan vuosikymmenen merkittävin muutos teknologian kentällä, tai ainakin sen alku. Viime vuoden aikana erilaiset tekoälyä hyödyntävät sovellukset ja järjestelmät yleistyivät huomattavasti, ja entistä kehittyneempiä tekoälyjä tuli laajemman yleisön saataville. Tämä voidaan katsoa alkaneen jo vuoden 2022 lopulla, kun ensimmäinen massiivista huomiota saanut tekoälysovellus ChatGPT julkaistiin vapaasti käytettäväksi. Tämän myötä sekä tekoälyyn kohdistuva kiinnostus, että etenkin ChatGPT:n kaltaisten generatiivisten tekstiä tuottavien tekoälyn käyttökohteita keksitiin jatkuvasti lisää. Näille sovelluksille kehitettiin sekä yleishyödyllisiä käyttötarkoituksia esimerkiksi tiedonhakuun tai koodaamiseen, mutta samalla myös rikollinen toiminta kehittyi esimerkiksi kalasteluviestien kehityksen tai tietoturva-aukkojen etsimisen suhteen. Työkaluihin liittyi myös merkittäviä ongelmia esimerkiksi plagioinnin ja tekijänoikeuksien osalta. Sekä ChatGPT:n että muiden tekoälysovellusten väärinkäyttöä pyrittiin estämään muokkaamalla sovellusta sen mukaan, mitä rikollisia käyttötarkoituksia sille keksittiin, mutta tämä harvoin onnistui, sillä pahantahtoiset toimijat joko keksivät tapoja ohittaa rajoitukset tai kehittivät samaan teknologiaan pohjautuvia täysin rajoituksettomia omia sovelluksia. Onkin hyvä ymmärtää, että uuden teknologia-aallon tullessa on käytännössä mahdotonta rajata sen käyttö vain lailliseen tai moraalisesti hyväksyttävään toimintaan, sillä rikolliset löytävät aina tavan hyödyntää sitä.

Tekoälyn potentiaalista saatiin kuluneen vuoden aikana maistiaisia sekä kyberturvallisuuden edistämisen että uhkatoimijoiden toiminnan kehityksen muodossa. Tekoälyä onnistuttiin hyödyntämään kyberturvan valvonnan automatisoinnissa, koodissa olevien virheiden tunnistamisessa ja entistä uskottavampien kalasteluviestien luomisessa. Koodin heikkouksien arviointi toimi myös tietoturva-asiantuntijoiden lisäksi rikollisten työkaluna, sillä tekoäly ei tiedä aiotaanko sen löytämiä aukkoja tietoturvassa paikata vai hyödyntää hyökkäyksessä. Vaikka viime vuonna yleistyneet tekoälyn eri sovellutukset ovatkin jo nyt hyvin kehittyneitä ja niillä potentiaalia sekä kyberturvallisuuden edistämiseen että uhkatoimijoiden operaatioiden kehitykseen, on oletettavaa, että tekoälystä saatavan hyödyn ja samalla teknologian merkityksen kanssa ollaan vielä alkuvaiheessa. Vielä tällä hetkellä tekoälyt ovat rajautuneet suhteellisen tarkasti vain yhdenlaiseen toimintaan, esimerkiksi tekstiä tuottava generatiivinen tekoäly ei osaa voittaa ihmistä shakkipelissä tai luoda uskottavia videoita tai kuvia, vaikka nämä kaikki ovat toimintoja, joissa tekoälyä voidaan tehokkaasti hyödyntää.

Vaikka tekoäly veikin valtaosan huomiosta teknologian kentällä ei silti tule unohtaa, että myös muilla rintamilla tapahtui muutoksia. Kilpailu mikrosiruista ja tulevaisuuden teknologian herruudesta jatkui Yhdysvaltojen ja Kiinan välillä ja Venäjä joutui yhä suurempiin vaikeuksiin kauppapakotteiden ja länsimaisesta teknologiasta irtautumisen vuoksi. Teknologiariippuvuus, jota suurvallat yrittävät ympärilleen levittää on yhä merkittävä ilmiö. Tietotekniikan jatkuvasti kasvattaessa merkitystään yhteiskuntien toiminnassa sillä, joka hallitsee mikrosirujen tuotantoa, tulee olemaan merkittävä valta-asema kansainvälisen politiikan kentällä. Tällä hetkellä vaikuttaa siltä, että Yhdysvallat on niskan päällä sirusodassa, mutta tulevaisuudessa esimerkiksi kvanttiteknologian tai tekoälysovellusten kehityskyky voi muokata tätä asetelmaa.

2. VUODESTA 2023 HALUAMME KOROSTAA

2.1. Miten kybersota kehittyi vuoden 2023 aikana

Kybersodankäynnistä ja sen määrittelystä on puhuttu paljon etenkin sen jälkeen, kun Venäjä hyökkäsi Ukrainaan vuonna 2022. Maataistelujen lisäksi Venäjä kiihdytti aggressiota myös kyber- ja informaatioulottuvuudessa. Vuoden 2023 aikana kybersodankäynti jatkui aktiivisena ja sai monia uusia ulottuvuuksia, niin Ukrainassa kuin muuallakin maailmalla. Vuosi 2023 osoitti viimeistään sen, miten kybersota on edelleen vaikeasti määriteltävä käsite, koska kybertoimintaympäristö ei varsinaisesti tunnista mitään valtiollisia tai muitakaan rajoja. Tämä on konkretisoituinut myös haasteena saattaa kybersotarikollisia vastuuseen teoistaan.

Informaatioulottuvuudessa kybersotaa käydään etenkin liittolaisuuksista, uskottavuudesta sekä henkisestä yliotteesta. Informaatio-operaatioilla ja kyberhyökkäyksillä pyritään vaikuttamaan esimerkiksi siihen, miten siviiliväestö kokee käynnissä olevan fyysisen sodan. Suurvallat hyödyntävät informaatioulottuvuutta oikeuttaakseen omaa toimintaansa ja saamaan muiden suurvaltojen toiminnan näyttämään vähintäänkin epäilyttävälle. Kybersodankäyntiin on vuonna 2023 kuulunut myös eräänlainen kilpavarustelun kulttuuri, jossa julkisesti on tuotu esille oman valtion kyberkapasiteettia. Tästä esimerkkinä on Yhdysvallat, joka näkyvästi ilmoitti kasvattaneensa maan digitaalisten taistelujoukkojen roolia maan ulkopuolelta tulevia vaikuttamispyrkimyksiä vastaan. Kiinan taas kerrottiin kehittäneen uudenlaista, satelliitteja kaappaavaa kyberasetta, mikä pakottaa muut suurvaltiot luonnollisestikin vastaamaan tähän haasteeseen. Kiina on korostanut paljon sitä, miten etenkin informaatioulottuvuudella on keskeinen asema maan sotilasstrategiassa ja ulkomaisen vaikuttamisen torjumisessa sen verkkoympäristöstä.

Kybersodassa kohteet ja toiminnan muodot vaihtelevat sykleittäin. Kuten fyysisessä sodankäynnissä, myös kybersodassa aktiivisten jaksojen välissä on usein vaihtelevan pituisia valmisteluvaiheita. Esimerkiksi Ukrainan sodassa ehdittiin vuonna 2023 puolin ja toisin oppimaan toisen osapuolen toimintatavoista, mikä taas pakotti toisen osapuolen muuntelemaan hyökkäysmenetelmiä myös kybertoimintaympäristössä. Venäjän ja Ukrainan välisessä kybersodassa myös korostui etenkin erilaisten ulkopuolisten toimijoiden hyödyntäminen. Iskujen toteutus onkin uusissa kybersodankäynnin muodoissa laajasti ulkoistettu asevoimien ja viranomaistahojen sijaan hallinnosta irrallisille kyberrikollisryhmille, jotka kykenevät aktivoitumaan hyvinkin nopeasti. Erilaisten rikollisryhmien ja ideologisten hakkeriryhmien hyödyntäminen kybersodankäynnissä säästää usein valtion omien kyberaseiden käyttöä kaikista kriittisempiin kohteisiin ja tarkemmin suunniteltuihin iskuihin.

Hybridisodankäynti on ylipäätään globaalisti lisääntynyt, mistä kertoo kyberhyökkäysten määrän kasvu myös valtioihin, jotka eivät suoranaisesti ole liittyneet mihinkään sotatoimiin. Myös esimerkiksi Kiina mieltää kybervoiman keskeiseksi osaksi hybridisodankäynnin konseptiaan ja monet sen viimeaikaisista kyberoperaatioista voidaankin nähdä varautumisena Taiwanin operaatioon. On todennäköistä, että huomattava määrä kehittyneimmästä valtiollisesta kybertoiminnasta tapahtuu edelleen suljettujen ovien takana, joista ei julkisuuteen tule edelleenkään tietoa. Taustalla tapahtuu myös paljon valtiojohtoista kybervakoilua ja tiedonhankintaoperaatioita, joista ei tiedoteta. Yksi kybersodankäynnin muutoksista on ollut valtioiden suhtautuminen maahan kohdistuviin kyberhyökkäyksiin, joihin pyrittiin vuoden 2023 aikana reagoimaan entistä nopeammin. Se on luonnollisesti kasvattanut riskiä siihen, että kybervaikuttamiseen vastataan ensioletuksen perusteella, ilman täyttä varmuutta tekijästä. Tämä puolestaan voi lisätä konfliktien määrää vähintään kybertoimintaympäristössä. Tulevaisuudessa yhä enemmän suunniteltuihin kineettisiin sotatoimiin ja terrori-iskuihin tulee liittymään mukaan myös kybervoiman käyttö.

Lähteet sivulla 41

2.2. Haktivismin nousu

Vuoden 2023 aikana haktivistien ja ideologisesti toimivien ryhmien rooli kyberhyökkääjinä on korostunut entisestään. Tämä on näkynyt myös Ukrainan sodassa, jonka myötä joukkoistaminen on ottanut askelia eteenpäin. Ukrainan puolella sotiva It-army of Ukraine on jatkanut toimintaansa ja koordinoinut muun muassa palvelunestohyökkäyksiä Venäjää vastaan, toisella puolella samaa ovat tehneet venäläismieliset haktivistit.

Tilanne ei kuitenkaan rajoitu pelkästään Ukrainan ja Venäjän väliseen sotaan, vaan myös esimerkiksi intialaiset kybervapaaehtoiset ovat suorittaneet iskuja poliittisista syistä. Vapaaehtoisten rooli on nähty myös Gazan sodassa, jossa molemmat osapuolet ovat saaneet vapaaehtoistukea. Nyrkkisääntönä tuntuu olevan, että moderneissa konflikteissa, olkoon konflikti poliittinen, diplomaattinen tai sotilaallinen, myös vapaaehtoiset ideologisesti motivoituneet hyökkääjät osallistuvat siihen, ikään kuin ulkopuolelta. Tästä on myös tilastollista näyttöä. Kyberanalytiikkafirma CloudSEKin tutkimuksen mukaan ideologisesti motivoituneiden kyberhyökkäysten määrä muodosti jopa 35 % kyberhyökkäyksistä huhti-toukokuussa 2023. Muutos on ollut nopea, sillä globaalisti niiden määrän on niiden arvioitiin olleen vain 1 % vuonna 2021.Vaikka lukuihin on syytä aina suhtautua terveellä epäilyksellä, on ideologisten hyökkäysten kasvu monien asiantuntijoiden tunnustama ja havaitsema asia.

Haktivistien ja ideologisesti motivoituneiden hyökkääjien suosimia hyökkäystapoja ovat olleet palvelunestohyökkäykset ja verkkosivuihin kohdistuva ilkivalta. Nämä ovat suhteellisen matalan tason toimintaa, mutta tilanne voi muuttua, sillä ryhmittymien välisen yhteistyön voi kasvaa ja sitä myötä muuttua muuttua vaarallisemmaksi ja edistyneemmäksi. Organisointi ja samanmielisten rekrytointi on tänä päivänä aiempaa helpompaa. Jos vuosia on kuviteltu hakkerien toimivan pääasiassa pimeässä ja syvässä verkossa, vuonna 2023 julkisesti saatavilla olevat kanavat, erityisesti Telegram, kasvattivat suosiotaan viestinnän ja toiminnan koordinoinnin välineenä. Haktivismi vaikuttaakin tulleen jäädäkseen ja teknologioiden kuten tekoälynkehitys tulee todennäköisesti helpottamaan vapaaehtoisten ja teknisesti vähemmänkin taitavien osallistumista kyberkamppailuihin. Vastaisuudessa voidaankin olettaa sekä haktivistien suorittamien matalantason operaatioiden että monimutkaisempien yhteisoperaatioiden määrän kasvua.

3. OTA MUKAAN VUODELLE 2024

3.1. NIS2 - laki kyberturvallisuuden riskienhallinnasta tulossa

NIS2-kyberturvallisuusdirektiivin implementointia kansalliseen lainsäädäntöön tehdään kiihtyvällä vauhdilla. Laki kyberturvallisuuden riskienhallinnasta on tulossa voimaan vuoden 2024 lokakuussa. Lain soveltamisalaan kuuluvien organisaatioiden tulee ilmoittautua valvovan viranomaisen ylläpitämään toimijaluetteloon 1.1.2025 mennessä. Julkisen sektorin puolella direktiivin täytäntöönpano hoidetaan muuttamalla tiedonhallintalakia.

Lain myötä toimijoille tulee yleinen kyberturvallisuuden riskienhallintavelvoite. Toimijoiden on tunnistettava, arvioitava ja hallittava riskejä toteuttamalla riittävät turvallisuus- ja riskienhallintatoimenpiteet. Johto on vastuussa riskienhallinnan toimintamallin toteuttamisesta. Lain myötä sen piiriin kuuluville organisaatioille tulee myös velvoite raportoida viipymättä merkittävistä poikkeamista valvovalle viranomaiselle. Riskienhallinta- ja raportointivelvoitteiden sekä toimijaluetteloon ilmoittautumisen laiminlyönnistä voidaan määrätä hallinnollinen seuraamusmaksu.

Lain tulemiseen kannattaa ryhtyä valmistautumaan viimeistään nyt. Riskienhallinnan toimintamallin luominen tai olemassa olevan hallintaympäristön parantaminen kyberturvallisuuden huomioonottamiseksi vie aikaa. Samoin laissa määriteltyjen, kyberriskien hallintakeinojen vähimmäisvaatimusten täyttäminen on huolellista suunnittelua ja määrätietoista työtä vaativa projekti. Konkreettiseen alkuun kymmenen vähimmäisvaatimuksen toteuttamisessa pääsee lain ja asiamukaiset viitekehykset (ISO 27001, kybermittari) huomioivalla puuteanalyysilla.

Lähteet sivulla 41

3.2. Kriittinen infrastruktuuri edelleen kasvaneen kiinnostuksen kohteena

Kasvanut huoli kriittiseen infrastruktuuriin kohdistuvasta kyberuhasta oli läsnä koko 2023 vuoden enemmän kuin koskaan aiemmin. Kriittiseen infrastruktuuriin kohdistuneet kyberhyökkäykset ja niiden yritykset kasvoivatkin merkittävästi. Vaikutuksiltaan laajoja ja paljon huomiota saaneita hyökkäyksiä nähtiin huomattavasti aiempaa enemmän. Joukkoon mahtui useita kansainvälisesti merkittäviä satamia sekä terveydenhuollon yksiköitä, jotka kasvavassa määrin joutuivat muun muassa palvelunestohyökkäysten ja kiristyshaittaohjelmahyökkäysten kohteiksi. Suomessakin asia konkretisoitui viimeistään Itämeren merenalaisiin tietoliikennekaapeleihin sekä Suomen ja Viron väliseen kaasuputkeen kohdistuneen sabotaasin myötä.

Kriittinen infrastruktuuri pysyy edelleen monin tavoin houkuttelevana kohteena kybervaikuttamiselle. Iskujen tai niistä johtuvien häiriöiden laajat vaikutukset koko yhteiskuntaan houkuttelevat sekä taloudellisesti motivoituneita rikollisia että valtiollisia tahoja, jotka usein saattavat toimia myös yhteistyössä keskenään. Valtiollinen vaikuttaminen on saatettu piilottaa näennäisen rikollisen tai taloudellisen motiivin taakse. Kriittiseen infrastruktuuriin kohdistuvilla hyökkäyksillä on myös kybermaailmassa hyvin harvinainen mahdollisuus aiheuttaa merkittävää fyysistä vahinkoa, eivätkä iskujen heijastevaikutukset rajoitu koskemaan vain yhteistyökumppaneita tai asiakkaita. Esimerkiksi sähköverkkoon tai julkiseen liikenteeseen kohdistuvalla iskulla on myös huomattava informaatiovaikutusarvo, joka voi palvella ideologisia tavoitteita epävarmuuden ja pelon kylvämisessä. Iskut pyritään usein myös ajoittamaan sellaiseen hetkeen, jolla saadaan kaikista suurin vaikutus kohde yhteiskunnassa.

Kriittiseen infrastruktuuriin kohdistuvat iskut voitiin vuoden 2023 aikana yhdistää moniin laajakirjoisiin hybridivaikutuskampanjoihin, joita etenkin Venäjä toteutti. Valtiolliset toimijat pyrkivätkin usein lamauttamaan yhteiskunnan kriittisiä toimintoja osana hybridioperaatioita. Etenkin energiasektoriin kohdistuneet kyberhyökkäykset on yhdistetty juuri hybridisodankäyntiin ja valtiolliseen toimintaan. Myös terveydenhuollon sektoriin kohdistuvat iskut lisääntyivät eritoten siksi, että on yksi yhteiskunnan kaikista kriittisin osa-alue. Terveydenhuolto on myös taloudellisesti hyvin kannattava kohde kyberrikollisille. Energia-, logistiikka ja terveyssektorin ohella uusiksi merkittäviksi kohteiksi ovat tulleet mediasektori sekä lainvalvontaviranomaiset. Esimerkiksi mediasektoriin kohdistuvien hyökkäysten tavoitteena voi olla informaatiotilaan vaikuttaminen ja mahdollisten valeuutisten levittäminen. Venäjän lisäksi aktiivisia valtiollisia toimijoita ovat viime vuosina olleet Kiina ja Pohjois-Korea.

Usein kriittiseen infrastruktuuriin kohdistuvilla iskuilla on myös lukuisia heijastevaikutuksia muihin yhteiskunnan osa-alueisiin. Kybermaailman keskinäisriippuvuudet ovatkin teema, josta on puhuttu vuosia. Tällä tarkoitetaan esimerkiksi tilanteita, joissa kybermaailman häiriöt leviävät tehokkaasti organisaatioiden ja toimialojen rajojen yli. Alihankkijaa voidaan käyttää vektorina laajan vaikutuksen saamiseksi ja lunnasvaatimuksen kohteena voi olla yrityksen oman datan sijaan asiakkaille tuotettavan palvelun keskeytyminen ja sitä myötä syntyvä haitta. Hyökkäysten aiheuttamien häiriöiden vaikutukset voivat myös levitä tahattomasti ja etenkin kansallisesti merkittävien toimijoiden kokemat iskut tuntuvat laajalti. Kyberhyökkäykset kriittiseen infrastruktuuriin tulevat varmasti lisääntymään myös vuonna 2024 ja epäilemättä hyökkäysmenetelmät tulevat monipuolistumaan ja tehostumaan. ■

LÄHTEET

KANSAINVÄLINEN KYBERYMPÄRISTÖ:
Cyberwatch Finlandin viikkokatsaukset vuodelta 2023

KYBERRIKOLLISUUS:
Cyberwatch Finlandin viikkokatsaukset vuodelta 2023
What is triple extortion ransomware? | Definition from TechTarget
WS_Professionalisation_of_CyberCrime_EN.pdf (withsecure.com)

TEKNOLOGIA:
Cyberwatch Finlandin viikkokatsaukset vuodelta 2023

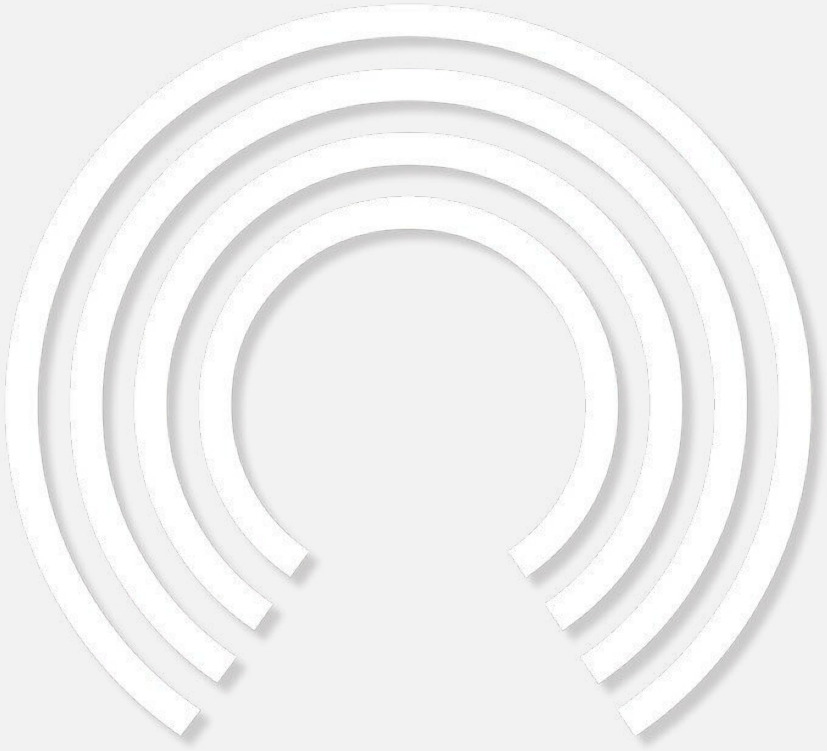
MITEN KYBERSOTA KEHITTYI VUODEN 2023 AIKANA:
Cyberwatch Finlandin viikkokatsaukset vuodelta 2023

HAKTIVISMIN NOUSU
Cyberwatch Finlandin viikkokatsaukset vuodelta 2023
https://securitybrief.asia/story/surge-in-hacktivism-aligns-with-geopolitical-tensions-in-2023
https://www.itbrew.com/stories/2023/09/12/new-report-details-rise-in-hacktivism-motivations-for-attacks

NIS2
NIS2-direktiivi (EU) 2022/2555
Hallituksen esitysluonnos eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

KRIITTINEN INFRASTRUKTUURI EDELLEEN KASVANEEN KIINNOSTUKSEN KOHTEENA:
Cyberwatch Finlandin viikkokatsaukset vuodelta 2023

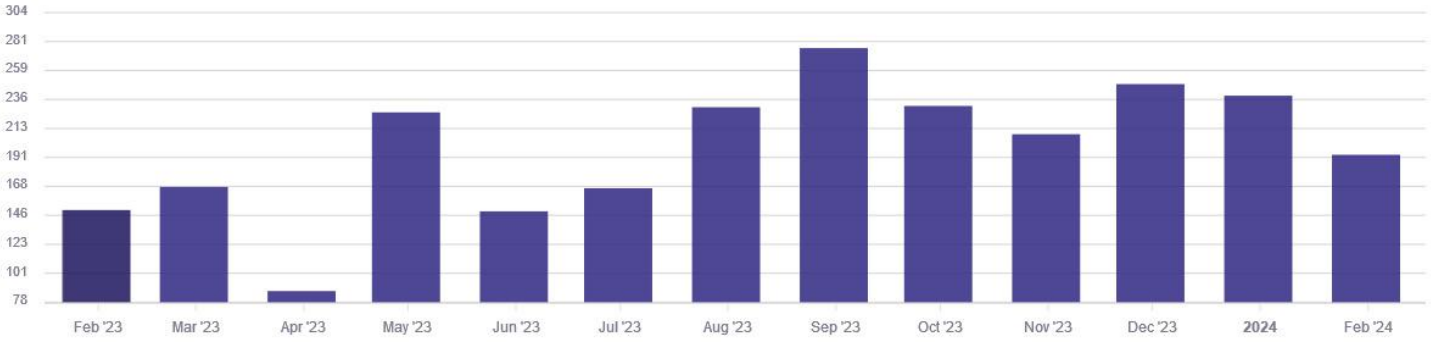
Cyberwatch Finland



UHKATIEDUSTELUSEURANTA

Cyberwatch Finland julkaisee uhkatiedusteluseurannan, johon on koottu viimeisen kuukauden ajalta merkittävimpiä kyberhyökkäyksiä sekä tietoa aktiivisimmista uhkatoimijoista ympäri maailman. 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

LURIE LASTENSAIRAALA CHICAGO

AJANKOHTA: 31.1.2024

KUVAUS: Lurie lastensairaala Chicagossa kärsi lunnashaittatoimija Rhysidan kyberhyökkäyksen tammi-helmikuun vaihteessa. Sairaala on Yhdysvaltain johtava lasten akuuttihoitolaitos ja hoitaa vuosittain yli 200 000 lasta. Ryhmä väittää saaneensa haltuun 600 GB dataa ja pyytää siitä 60 bitcoinia lunnaaksi.Tätä kirjoittaessa yhden bitcoinin arvo on noin 58 000 euroa eli lunnasvaatimus on noin 3,5 miljoonaa euroa.

TEKIJÄ: Rhysida

MOTIIVI: Taloudellinen

VAIKUTUKSET: Sairaalan IT-järjestelmät jouduttiin siirtämään offline-tilaan ja joitain hoitotoimenpiteitä jouduttiin lykkäämään. Lääkärit joutuivat vaihtamaan kynään ja paperiin reseptejä kirjoittaessa. Nyt noin kuukausi iskun havaitsemisen jälkeen sairaalan IT-palvelut ovat edelleen osittain alhaalla ja palveluhäiriöt vaikuttavat joihinkin toimintasegmentteihin. Reseptit kirjoitetaan edelleen käsin ja joitain potilastapaamisia joudutaan perumaan ja uudelleen ajoittamaan akuuteimpien tapausten tieltä. Lunnasvaatimus on edelleen aktiivinen.

MERKITTÄVIMPIÄ KYBERISKUJA JA -KAMPANJOIA

INFOSYS MCCAMISH SYSTEMS LLC JA BANK OF AMERICA -TIETOVUOTO

AJANKOHTA: 3.-24.11.2023, julkisuuteen 1.2.2024
KUVAUS: Noin 57 tuhannen Bank of American asiakkaan tietoja päätyi uhkatoimijalle pankin vakuutuskumppaniin kohdistuneen tietomurron seurauksena. Vuotaneita tietoja ovat voineet olla muun muassa asiakkaiden nimet, fyysiset- ja sähköpostiosoitteet, syntymäajat sekä sosiaaliturvatunnukset.
TEKIJÄ: Lockbit
MOTIIVI: Taloudellinen
VAIKUTUKSET: Ihmetystä on aiheuttanut tapahtumasta ilmoittaminen näinkin pitkään tapahtuneen tietomurron seurauksena. Sen on arveltu mahdollisesti rikkovan lakia ja on aiheuttanut mainehaittaa organisaatioille. Tavallisen asiakkaan kannalta vuotaneet tiedot voivat altistaa esimerkiksi identiteettivarkauksille. Korvauksena Bank of America onkin tarjonnut asiakkailleen ilmaista kahden vuoden palvelua identiteettitietojen suojelemiseksi.

BJUVIN KUNTA

AJANKOHTA: 24.1.2024
KUVAUS: Akira Ransomware-niminen uhkatoimija on ilmoittanut hallussaan olevasta ruotsalaisen Bjuvin kunnan tietoja, jotka ryhmä uhkaa julkaista pimeässä verkossa. Data on todennäköisesti päätynyt ryhmän haltuun helmikuun alussa tapahtuneessa Ruotsiin kohdistuneessa tietomurtosarjassa. Tässä sarjassa pääuhrina oli Tietoevry, mutta iskun myötä myös satojen pienempien Tietoevryn palveluita käyttäneiden toimijoiden järjestelmiä altistui. Tarkkaa tietoa siitä miten Akira on pienen kunnan tietoja käsiinsä saanut ei kuitenkaan ole, eikä myöskään ryhmän omien väitteiden lisäksi käsitystä minkälaista dataa ryhmällä hallussaan on.
TEKIJÄ: Akira Ransomware.
MOTIIVI: Epäselvä, Akiran toimintatapoihin tyypillisesti kuuluu ransomware-ohjelman käyttö ja datan palauttamisella kiristäminen. Tässä tapauksessa Akira ei edes vaikuta vaativan lunnaita, vaan yksinkertaisesti uhkaa tietojen vuotamisella.
VAIKUTUKSET: Ei tarkkaa tietoa sillä on epäselvää minkälaista dataa Akiralla voi olla hallussaan. Mahdollisesti kyseessä on kuntalaisten henkilötietoja, sopimuksia ja taloustietoja ja näiden paljastuminen voi johtaa monien eri uhkien realisoitumiseen sekä kunnalle itselleen että siellä asuville tai toimiville yrityksille.

AKTIIVISIMPIA TOIMIJOITA

MOGILEVICH RANSOMWARE

KUVAUS: Helmikuussa 2024 ensimmäisen kerran havaittu rikollisryhmä. Ilmoittanut olevansa puhtaasti taloudellisesti motivoitunut toimija. Mainostaa itseään Ransomware-as-a-service (RaaS) toimijana, ja etsii aktiivisesti yhteistyökumppaneita muista hakkeriryhmistä.
VIIME AIKOJEN TOIMINTA: Ilmoittanut iskeneensä useisiin kohteisiin helmikuun aikana. Suurimpia kohteita ovat olleet pelivalmistaja Epic Games ja Irlannin puolustusministeriö. Molemmat tahot ovat tosin ilmoittaneet, että mitään iskua ei ole tapahtunut. Näiden lisäksi yksikään muista ryhmän itse ilmoittamien iskujen kohteista ei ole julkisesti myöntänyt hyökkäyksiä, eikä ryhmä ole julkaissut todisteita onnistuneista iskuista.
TOIMINTATAVAT JA TAKTIIKAT: Toisin kuin moni muu kiristystoimija, ei julkaise ”näytteitä” varastamastaan datasta. Tämä yhdistettynä verrattain mataliin lunnasvaatimuksiin on johtanut monet uskomaan, että ryhmän itse ilmoittamat iskut ovat valheellisia, ja varsinaisen kiristämisen sijaan ryhmä pyrkii matalilla lunnasvaatimuksilla ja uhkaavilla viesteillä painostamaan uhria maksamaan ilman että mitään dataa on edes kaapattu.

LOCKBIT

KUVAUS: Yksi tunnetuimmista ja suurimmista Ransomware as a Service (RaaS) - toimijoista. Myy kehittämäänsä lunnashaittaohjelmaa alihankkijoilleen, jotka tekevät varsinaiset lunnashaittaohjelma - hyökkäykset.
VIIME AIKOJEN TOIMINTA: Kärsi helmikuun aikana mittavia tappioita poliisiviranomaisten kansainvälisen iskun myötä. Ryhmän verkkopalvelut ja niitä pyörittävät dataserverit päätyivät viranomaisten haltuun ja näiden mukana runsaasti dataa, mukaan lukien lunnashaittaohjelmien purkuavaimia. Tämän lisäksi ryhmän hallinnoimia kryptovaluuttatilejä jäädytettiin. Ryhmän kärsimistä tappioista huolimatta, lunnashaittaohjelma-hyökkäyksiä toteuttavat alihankkijat näyttävät ainakin toistaiseksi tekevän lähes normaaliin tapaan iskuja. Tulevina kuukausina onkin hyvä seurata, miten tämä aktiivisuus kehittyy.
TOIMINTATAVAT JA TAKTIIKAT: Tätä kiristyshaittaohjelmaa käytetään tarkasti kohdennettuihin hyökkäyksiin, jotka estävät kohteen pääsyn tietokonejärjestelmään lunnaita vastaan.

CACTUS RANSOMWARE

KUVAUS: Haktivistiryhmä, joka on ollut aktiivinen ainakin vuoden 2023 maaliskuusta lähtien.
VIIME AIKOJEN TOIMINTA: Ryhmä iski helmikuussa hollantilaisen maatalous ja ruoantuotannon logistiikkayritys AB Texelin tietoverkkoihin. 1TB dataa on väitetysti kaapattu. Myös ranskalainen Schneider Electric sähkötekniikan laitteita ja komponentteja valmistava yhtiö kärsi helmikuun aikana ryhmän lunnashyökkäyksen. Tässä tapauksessa on väitetysti kaapattu 1,5TB yhtiön dataa. Maaliskuusta 2023 lähtien ryhmä on lisännyt yli 100 yritystä tai organisaatiota tietovuotosivustoonsa.
TOIMINTATAVAT JA TAKTIIKAT: Ryhmä hyödyntää ostettuja tunnistetietoja, kumppanuuksia eri haittaohjelmatoimijoiden kanssa, tietojenkalasteluhyökkäyksiä ja tietoturva-aukkoja. Ryhmä on hyödyntänyt muun muassa VPN ohjelmien haavoittuvuuksia.

KAUPALLISET VAKOILUOHJELMATOIMIJAT: CY4GATE, RCS LABS, IPS INTELLIGENCE, VARISTON IT, TRUEL IT, PROTECT ELECTRONIC SYSTEMS, NEGG GROUP JA MOLLITIAM INDUSTRIES

KUVAUS: Muun muassa Facebookin ja Instagramin taustalla olevat jättiyhtiö Meta julkisti helmikuussa uhkaraporttinsa, joka tarkastelee vuoden 2023 viimeisen neljänneksen tietoturvatapahtumia. Uutena havaintona yhtiö havaitsi kahdeksan uutta kaupallista vakoiluohjelmatoimijaa, jotka on rekisteröity Italiaan, Espanjaan ja Yhdistyneisiin Arabiemiirikuntiin.
VIIME AIKOJEN TOIMINTA: Yhtiöt ovat ottaneet kohteekseen iOS-, Android- ja Windows-laitteita, tarkoituksenaan saada pääsy laitteelle ja sitä myötä kohteen henkilökohtaisiin tietoihin.
TOIMINTATAVAT JA TAKTIIKAT: Yleisesti vakoiluohjelmia pidetään merkittävänä uhkana paitsi yksilöille, myös yhteiskunnille laajemmin. Autoritääriset valtiot ovat hyödyntäneen kaupallisia vakoiluohjelmia esimerkiksi oppositiopoliitikoiden vakoiluun. Useat vakoiluohjelmat voidaan toimittaa niin kutsutulla “zero click” -menetelmällä, mikä ei vaadi uhrilta tietoturvaerhettä tai jätä jälkiä laitteeseen. Nyt kyseessä olevat yhtiöt ovat tehostaneet toimia myös luomalla valeprofiilejasosiaaliseen mediaan sekä jakamalla saastutettua versiota WhatsAppista.

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

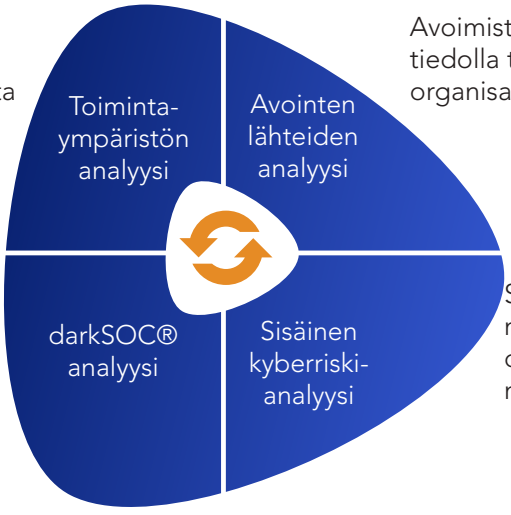
Olemme kokenut ja luotettu johdon neuvonantaja ja asiantuntija. Tuemme sinua kokonaisturvallisuuden, kyberturvallisuuden, sisäisen turvallisuuden asiakokonaisuuksissa ja kumppaniriskien hallinnassa. Työskentelymetodeinamme ovat muun muassa teema-alustukset, muistiot, työpajat ja skenaariotyöskentely.

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

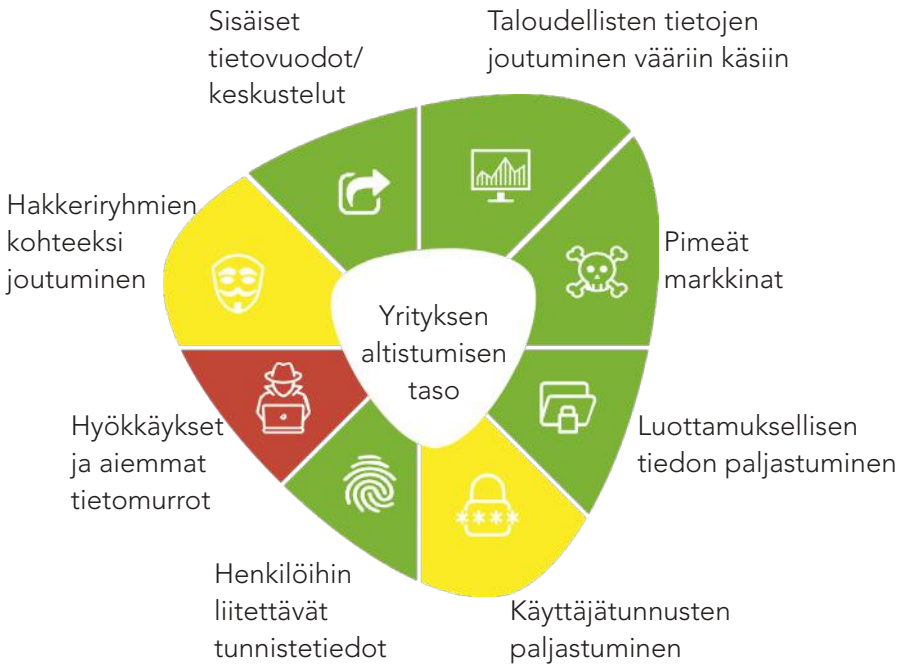
Tuotamme määrittelemästäsi teemasta, esimerkiksi tietystä toimialasta tai kohdemarkkinasta raportteja ja katsauksia: nykytilan arviointeja, uhka-arvioita, toimintaympäristöanalyyseja ja ennusteita

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 Puuteanalyysi

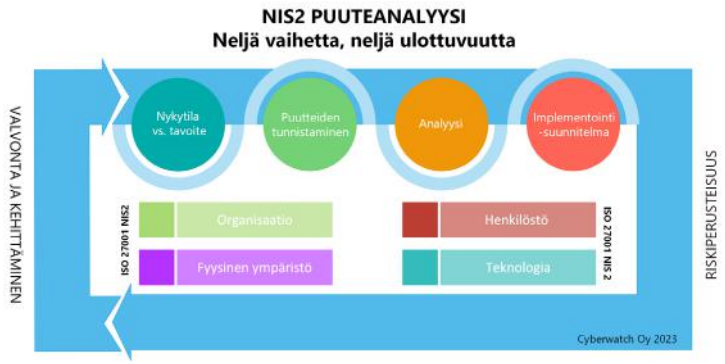
NIS2 kyberturvallisuus direktiivin tavoitteena on parantaa kyberturvallisuuden perustasoa EU:n alueella ja varmistaa kriittisten toimijoiden toiminnan jatkuvuus.
Direktiivi tuli voimaan 17.1.2023, jäsenmaissa aikaa laittaa asiat kuntoon 17.10.2024 mennessä.

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

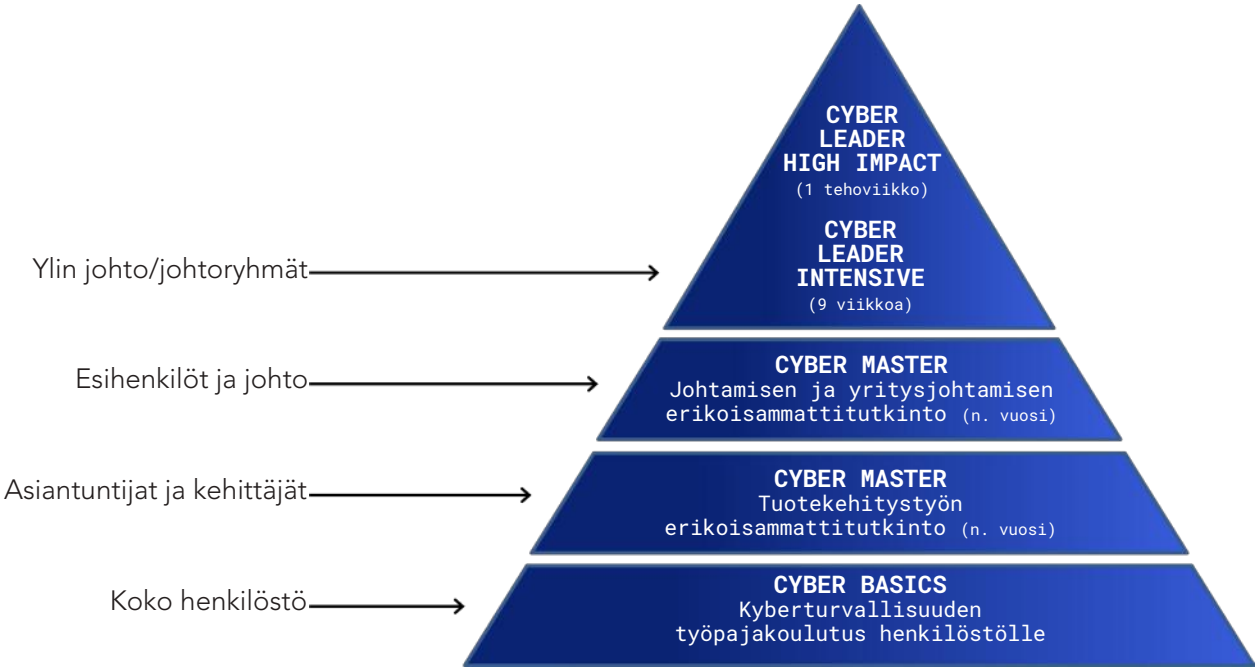
Koulutus ja osaamisen kehittäminen

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.



PALVELUMME

Forensiikkapalvelut

Väärinkäytösselvitykset ja erityistarkastukset

Avustamme organisaatiotasi taloudellisten väärinkäytösten, compliance-rikkomusten ja muun epäeettisen toiminnan estämisessä, tutkimisessa ja niihin liittyvissä korjaavissa toimenpiteissä. Tarjoamme käyttöönne riippumattoman asiantuntijuuden. Suoritamme toimeksiannon itsenäisesti jatkuvasti kommunikoiden tai tuemme toimeksiantajaa sen suorittamassa työssä. Meillä on laaja kokemusta tutkinta- ja tarkastustyöstä ja hallitsemme uusimpien säännösten määräykset menettelyvaatimuksista.

Taustaselvitykset

Selvitämme yritysten ja yrityshenkilöiden mainetta, integriteettiä ja toimintahistoriaa keräämällä ja analysoimalla tietoa päätöksenteon tueksi eri tilanteisissa, kuten yritysjärjestelyissä ja kolmansien osapuolten kanssa toimittaessa.

Riskienhallintapalvelut

Avustamme organisaatiotasi kokonaisvaltaisesti riskien tunnistamisessa, arvioinnissa ja hallinnassa.

Kokeneet asiantuntijamme hyödyntävät työssään uusimpia riskienhallinnan teknologioita.

Rahanpesuntorjunta

Tuemme organisaatiotasi rahanpesulain velvotteiden täyttämisessä.

Asiakkaan tunteminen
Know Your Customer (KYC)
Customer Due Diligence (CDD)

Rahapesun ja terrorismin rahoittamisen torjunnan tuki:
politiikat, ohjelmat, riskiarviot

Cyberwatch eWHISTLE-ilmoituskanava

Cyberwatch eWHISTLE- ilmoituskanavapalvelu tarjoaa vastuullisen, tietoturvallisen ja yksityisyydensuojan varmistavan ilmoituskanavan, jossa ilmoitusten käsittelylle, tutkinnalle ja päätöksenteolle on luotu selkeä ympäristö.

eWHISTLE on täyden palvelun paketti. Laadimme ilmoituskanavan käyttöönoton vaatimat ja sitä tukevat prosessit ja dokumentit, tuemme lakisääteisten velvoitteiden täyttämisessä ja käynnistämme ilmoituskanavan. Kanavan käyttöönoton jälkeen otamme halutessasi ilmoitukset puolestasi vastaan, teemme ensiarvion ja laadimme ehdotuksen jatkotoimenpiteistä.

Ilmoituskanavapalvelun teknisen alustan tuottaa suomalainen Easywhistle Oy. Järjestelmä on helposti saavutettava, turvallinen ja käyttäjäystävällinen. Järjestelmä on saatavana lukuisilla kielellä. Palvelun tuottava yritys on ISO 27001 sertifioitu ja kanava täyttää GDPR-vaatimukset. Sen palvelimet sijaitsevat EU:n alueella.

eWHISTLE

INTOHIMONA KYBERTURVALLISEMPI MAAILMA

Ota yhteyttä

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
ake@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi

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 at cybersecuritynordic.com

CYBER SECURITY NORDIC

29–30 October 2024
Helsinki Expo and Convention Centre

MESSUKESKUS
The real social media