Cyberwatch Finland

VIIKKOKATSAUS

46/2025

Teemakatsaus **CYBER SECURITY NORDIC**

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

Cyberwatch Finland

VIIKKOKATSAUS

46/2025

- Perinteiset Cyber Security Nordic –kyberturvallisuusmessut järjestettiin marraskuun alussa Helsingissä.

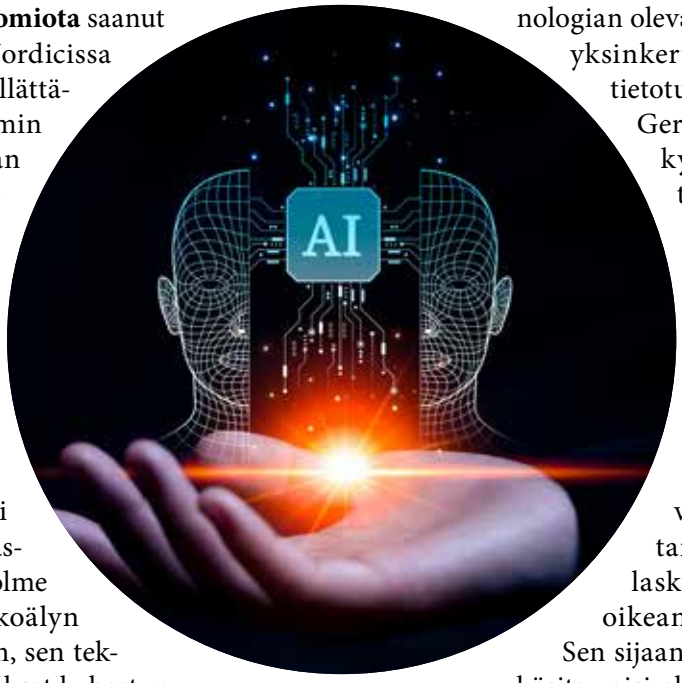
- Tapahtuma keräsi yli 2600 vierailijaa ja 75 näytteilleasettajaa. Tilaisuuden avasi puolustusministeri Antti Häkkänen ja paikalla oli yritysedustajien lisäksi muun muassa Viron elinkeinoministeri.

- Esityksissä käsiteltiin monipuolisesti eri kyberturvallisuuden teemoja, mutta tänä vuonna tekoälyn ja geopolitiikan merkitykset korostuivat.

Johdanto

Yksi pohjoismaiden suurimmista kyberturvallisuustapahtumista, Cyber Security Nordic, järjestettiin jälleen marraskuun alussa Helsingin messukeskuksessa. Tänä vuonna tapahtuma keräsi saman katon alle yli 2600 vierailijaa ja 75 näytteilleasettajaa, minkä lisäksi ohjelmassa oli kymmeniä asiantuntijapuheenvuoroja. Tapahtuman nimekkäitä puhujia olivat muun muassa Suomen puolustusministeri Antti Häkkänen, Viron elinkeinoministeri Erkki Keldo ja Taiwanin Suomen-lähettiläs Freddy Lim. Messujen avauspuheenvuorossaan ministeri Häkkänen käsitteli kokonaisturvallisuutta ja maailmanpolitiikan jännitteitä, muun muassa Ukrainan sodan kontekstissa sekä Kiinan ja Yhdysvaltojen välillä. Geopolitiikka ja maailmantilanne yhdessä tekoälyn kanssa muodostivatkin kaksi toistuvaa teemaa asiantuntijoiden esityksissä. Asiantuntijapuheenvuorojen lisäksi messuilla on merkittävä rooli kyberturva-alan toimijoiden, eli yritysten, viranomaisten ja asiantuntijoiden yhteenkokoajana. Sekä messukäytävillä että puheenvuoroissa läpikulkevana vireenä kulkikin ajatus siitä, että uhkien moninaistuessa kybermaailman toimijoiden yhteistyöllä on merkittävä rooli niihin vastaamisessa ja edun saamisessa uhkatoimijoihin nähden.

Tekoäly messujen kärkiteemana



Ylivoimaisesti eniten huomiota saanut teema Cyber Security Nordicissa oli tekoäly. Tämä ei ole yllättävää nykyisen tekoälybuumin keskellä, jossa teknologian uhkista ja mahdollisuuksista keskustellaan laajasti sekä Suomessa että ulkomailla. Messujen ohjelmistossa tekoäly mainittiin jopa 16 puheenvuoron otsikossa, ja vain harvoissa puheenvuoroissa tekoälyä ei käsitelty ollenkaan. Karkeasti tekoälyn vaikutusten tarkasteluun oli löydettävissä kolme selkeää näkökulmaa: tekoälyn vaikutukset yhteiskuntiin, sen tekninen toiminta ja vaikutukset kyberturvallisuuteen.

Yksi parhaista tekoälyn yhteiskunnallista vaikutuksia käsitelleistä puheenvuoroista oli Philip Stupakin puheenvuoro kansallisesta turvallisuuspolitiikasta ja tekoälystä. Hänen havaintojensa mukaan tekoälyn sääntely ja riskienhallinta ovat vielä kehittymässä, mikä aiheuttaa selkeitä haasteita yhdessä toimijoiden eritahtisuuden kanssa. Esimerkiksi yritykset haluaisivat edetä nopeasti tekoälyn kehityksessä ja käyttöönotossa, mutta vaikkapa EU:ssa sen sijaan kehitystä on pyritty jarruttelemaan regulaation keinoin. Tekoälyn vaikutukset ovat kuitenkin globaaleja, ja samoin merkittävimmät tekoäly-yritykset toimivat globaalisti. Stupak heittikin ilmoille ajatuksen siitä, onko jopa nykyinen suvereeneihin kansallisvaltioihin perustuva poliittinen järjestelmä muuttumassa tämän myötä. Samalla tekoälyllä on merkittävä vaikutus työmarkkinoilla, sillä se muuttaa erityisesti korkeasti koulutettujen työntekijöiden työtä. Osa tehtävistä katoaa nopeammin kuin uusia syntyy. Tämä aiheuttaa luonnollisesti haasteen, johon tulisi vastata. Yksi Stupakin esittämä mahdollinen ratkaisu olisi tekoälyn verottaminen. Tämä voisi tapahtua joko verottamalla tekoälyn käyttämiä resursseja kuten sähköä, tai sen tekemää työtä. Tärkeintä olisi, että ihmisen ja tekoälyn suhde olisi toisiaan tukeva.

Vaikka Stupak näki tekoälyn jopa yhteiskuntia ja globaalia järjestystä mullistavana teknologiana, useissa puheenvuoroissa huomautettiin tekoälyteknologian olevan lopulta jossain määrin yksinkertaista. Esimerkiksi sekä tietoturvatalo Fortinetin tutkija Geri Revay että offensiivista kyberturvallisuuskonsultointia tarjoavan Reversecin pääkonsultti Antti Laatikainen totesivat tekoälyn näkyvimpien nykyisten sovellusten, eli laajojen kielimallien (LLM) ja generatiivisen tekoälyn (generative ai), olevan lopulta vain matemaattisia malleja tai "ennustekoneita", jotka laskevat todennäköisyyksiä oikean sisällön tuottamiseksi. Sen sijaan agentti-AI:n (agentic ai) -käsite voisi olla hyödyllisempi tulevaisuudessa. Tässä mallissa tekoäly ei enää olisi työkalu, vaan itsenäinen toimija, joka pystyisi toimimaan ja tekemään päätöksiä ilman jatkuvaa ihmisten ohjausta. Tällä olisi vaikutusta myös kyberturvallisuuteen.

Kyberhyökkäyksissä tekoälyn käyttöä voisi kuvata kilpajuoksuksi hyökkääjien ja puolustajien välillä. Sekä Revay että Laatikainen nostivat esiin tekoälyyn itseensä kohdistuvien kyberhyökkäysten, kuten promp-injektioiden muodostaman uhkan. Niissä tekoälyä huijataan tuottamaan haitallista koodia ja siten mahdollistetaan kyberhyökkäys. Revay korosti myös tekoälyn kyvykkyyksiä sosiaalisessa manipuloinnissa, kuten tietojenkalasteluviestien ja syvävääreennösten luomisessa. Natosta ja hyökkäyssimulaatioista messuilla puhuneen Accenturen Olli Luotosen mukaan generatiivinen tekoäly onkin tällä hetkellä mukana noin joka kuudennessa kyberhyökkäyksessä.

Vaikka tekoälyä käsiteltiin useissa puheenvuoroissa sen luomien uhkien kautta, sisältyy sen käyttöönottoon myös mahdollisuuksia. Asiantuntijoiden mukaan tekoäly voi auttaa kyberpuolustajia haavoittuvuuksien löytämisessä ja esimerkkejä onkin tekoälyn löytämistä nollapäivähaavoittuvuuksista. Samalla tekoälyä voitaisiin hyödyntää muun muassa uhkatiedon jakamisessa, ja SOC-toiminnassa AI-agentit voisivat olla merkittävänä apuna. Vaikka kyberrikolliset ovat nopeita ja häikäilemättömiä omaksumaan uusia toimintatapoja, pitkällä aikavälillä teknologian kehitys voi kääntyä kyberpuolustajien eduksi.

Geopolitiikka näyttelee yhä suurempaa roolia myös kybermaailmassa

Tekoälyn lisäksi toisena kantavana teemana läpi koko messujen oli geopolitiikka. Aihetta käsiteltiin tai vähintäänkin sivuttiin monesta eri näkökulmasta, mutta kokonaisuudessaan selväksi tuli ainakin se, että geopolitiikka on yhä suuremmassa roolissa myös kybermaailmassa. Slovakialaisen ajatuspaja GLOBSEC:in tutkimusjohtaja Katarína Klingová havainnollisti, minkälaisia toimijoita Venäjä käyttää hyväkseen hybridivaikuttamisessa. Kuten jo monesti on todettu, Venäjällä länsimaihin kohdistuva kyberrikollisuus on paitsi hyväksyttyä, usein valtiojohtoista. Usein valmiiksi heikossa asemassa olevia ihmisiä houkutellaan mukaan toimintaan joko rahalla tai manipulaatiolla, ja sama pätee hybridivaikuttamisessa laajemminkin. Useimmiten värvätyt toimijat tulevat entisiltä Neuvostoliiton alueilta, mutta on myös olemassa esimerkkejä paikallisten toimijoiden kuten järjestäytyneen rikollisuuden hyödyntämisestä. Huomionarvoista on, että monet erityisesti fyysiseen sabotaasiin syyllistyneistä eivät tiedä toimivansa Venäjän hyväksi, ja vain 27 % on aiemmin tuomittu rikoksista.

Toinen erityisesti huomion keskipisteenä ollut kybervaikuttaja oli Kiina. Cyberwatch Finlandin Aapo Cederbergin, Freddy Limin ja Hybrid CoE:n Jukka Savolaisen paneelissa hybridisodankäynnistä Itämeren ja Taiwanin alueella nosti esiin Kiinan hybridioperaatioiden pääasiallisena tavoitteena olevan sabotoida ja vaikuttaa globaalisti. Taustalla on ajatus siitä, että epäjärjestyksessä olevia alueita on helpompi hallita. Historiaa tuntevat voivat havaita yhtäläisyyksiä roomalaisten ajatukseen divide et impera, eli hajota ja hallitse. Kiinan motivaattorina toimii kilpailu maailman herruudesta erityisesti Yhdysvaltojen kanssa. Kiinan uhka on syytä ottaa vakavasti myös Euroopassa, sillä vaikka Eurooppa onkin huomattavasti merkittävämpi kohde Venäjälle, on Kiinalla uhkatoimijoista kaikkein suurin talous ja edistynein teknologia. Vaikka sen päähuomio onkin lähialueilla, sillä on tarpeen tullen kyky toimia myös Euroopassa.

Samalla on hyvä muistaa, kuten Taiwanin lähettiläs Freddy Lim totesi, että nykymaailmassa kieli ja kulttuuri eivät enää tarjoa samanlaista suojaa pienille valtioille kuin aiemmin. Taiwanissakin laskettiin vielä kymmenen vuotta sitten maan olevan huomattavasti keskimääräistä vaikeampi kohde hybridivaikuttamiselle näistä seikoista johtuen, mutta tilanne on sittemmin ratkaisevasti muuttunut. Suomi on täysin samassa asemassa, ja se tulisi ottaa nykyistä paremmin huomioon. Messujen puheenvuoroissa korostettiinkin moneen kertaan, että suuren toimijan laaja-alaiseen vaikuttamiseen vastaaminen vaatii ennen kaikkea yhteistyötä paitsi eri valtioiden, myös yksityisen ja julkisen sektorin sekä järjestöjen kesken.

Geopolitiikka liittyy kybermaailmaan myös teknologisen kehityksen kautta. Esiin nousi ennen kaikkea huoli internetin sirpaloitumisesta eli siitä, että jokin maantieteellinen alue irrotettaisiin internetistä kokonaan. Käytännössä se tarkoittaisi, että kyseisellä alueella otettaisiin käyttöön tietoverkko, joka ei ole yhteensopiva maailmanlaajuisesti käytössä olevan internetin kanssa. ICANN:in (Internet Corporation for Assigned Names and Numbers) edustajan mukaan tämän uhkakuvan takana on kolme tekijää: politisaatio, geopoliittinen epävakaus sekä uudet teknologiat.

Politisaation osalta erityisen huolestuttavaa on monin paikoin vallalla oleva pyrkimys digitaaliseen itsemääräämisoikeuteen. Vaikka ajatus sinänsä on kannatettava, on sitä tavoiteltaessa usein esitetty toimia, jotka voisivat johtaa internetin sirpaloitumiseen. Sama pätee myös lainsäädäntöön ja esimerkiksi EU:n regulaatioon. ICANN kritisoi erityisesti pyrkimyksiä vastata sisältötason ongelmiin internetarkkitehtuuriin puuttumalla, mikä johtaisi sirpaloitumiseen. Geopoliittisesta epävakaudesta puhuttaessa esimerkiksi nostettiin Ukrainan pyyntö sulkea venäläiset internet-domainit, kuten .ru-päätteiset sivustot helmikuussa 2022. Pyyntöön ei voitu ICANN:in epäpoliittisen luonteen vuoksi suostua, mutta vastaavat tapaukset luovat pohjaa sirpaloitumiselle. Myös uudet teknologiat, kuten Huawein kannattama "New IP", voivat johtaa sirpaloitumiseen, mikäli maat ovat erimielisiä siitä, mitä teknologiaa tulisi käyttää. Usein tässäkin on takana geopoliittisia intressejä saada omalle teknologialle hallitseva asema.

Yhteenveto

Kyberturvallisuusmessuille tuntuu joka vuosi muodostuvan jokin kantava teema: vuonna 2023 se oli Ukrainan sota ja viime vuonna NIS2-direktiivi ja kyberregulaatio. Tänä vuonna selvänä keihäänkärkenä toimi tekoäly. Sen lisäksi, että se oli läsnä monissa esityksissä, tekoäly näkyi myös messupisteillä. Vaikutti siltä, että jokainen paikalle tullut halusi tuoda esiin omaa toimintaansa nimenomaan tekoälyn kautta. Vaikka geopolitiikka ei aivan yhtä näkyvästi esillä ollutkaan, kulki se tekoälyn rinnalla puheenvuoroissa molempina päivinä. Niiden lisäksi messuilla käsiteltiin kyberrikollisuutta sekä siihen varautumista ja vastaamista. Kyberhyökkäyksiin varautumista ja reagointia käsiteltiin sekä teknisestä että strategisesta näkökulmasta. Mielenkiintoista oli lisäksi kuulla uusimpia lukuja kansalaisten luottamuksesta ja käsityksistä liittyen digitaalisiin työkaluihin. Karkeasti ottaen voidaan sanoa, että monet kyllä luulevat osaavansa toimia digimaailmassa turvallisesti, vaikka näin ei todellisuudessa olekaan. Eniten huolta kansalaisten parissa herättää messujen kantavan teeman mukaisesti tekoälyn nopea kehitys. Messut ovatkin kenties paras paikka aistia vallalla olevaa tunnelmaa, sillä osallistujien suurimmat huolenaiheet tuntuvat kiteytyvän kerta toisensa jälkeen messujen teemaksi. Onkin mielenkiintoista nähdä, mikä muodostuu seuraavan vuoden messujen pääteemaksi.

Tavoitteena kyberkyvykkäämpi maailma

Ota yhteyttä

Cyberwatch Oy | Nuijamiestentie 5 C | 00400 Helsinki, Finland
aapo@cyberwatchfinland.fi | info@cyberwatchfinland.fi | 040 500 8177