Strategisen kyberturvallisuuden erikoisjulkaisu

Cyberwatch Finland

MAGAZINE 2/2023

UKRAINAN SOTA MUUTTAA KYBERMAAILMAA

DIGITAALISTEN TAITOJEN PARANTAMISTA PAREMMAN EUROOPAN PUOLESTA

KYBERSOTA VENÄLÄISIN SILMIN

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

SISÄLLYS

2/2023

Cyberwatch Magazine

Strategisen kyberturvallisuuden erikoisjulkaisu

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

TOIMITUS
Päätoimittaja
Aapo Cederberg

Toimitussihteeri
Elina Turunen
elina@cyberwatchfinland.fi

ULKOASU JA TAITTO
Elina Turunen
elina@cyberwatchfinland.fi

KUVITUS
Unsplash
Pixabay
Shutterstock

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

PAINO
Scanseri Oy, Helsinki

Pääkirjoitus

UKRAINAN SOTA MUUTTAA KYBERMAAILMAA

// Aapo Cederberg

Läpi maailman historian sodat ovat muuttaneet historian kehityskulkuja ja olleet enemmän tai vähemmän uuden aikakauden alku. Ukrainan sota romuttaa nykyinen Euroopan turvallisuusarkkitehtuuri. Suomessa turvallisuusympäristö on pysyvästi muuttunut, ja hyvien suhteiden palauttamisen Venäjän kanssa on vaikeaa ja vaatii varmasti pitkän ajan. Natojäsenyys on kuitenkin vahvistanut kansallista turvallisuuttamme emme ole yksin, vaan puolustusliiton jäsen ja myös osa liittokunnan kyberpuolustusta.

Nämä poliittiset muutostekijät näkyvät kybermaailmassa, vaikka Ukrainan merkityksestä kybermaailman muutoksessa puhutaan suhteellisen vähän. Jo tässä vaiheessa voidaan nähdä ainakin kolme merkittävää muutosta:

1 Kyberstrategioiden konseptit ovat muuttumassa hyökkäykselliseksi. Vihollisen ja rikollisten kybervoimaan pyritään aktiivisesti heikentämään aktiivisilla kyberoperaatioilla.

2 Kyberrikollisuus on jakautunut joko Ukrainaa tukevaan tai vastustavaan toimintaan. Taloudellisten ja valtiollisten päämäärien yhdistämien on entistä ilmeisempää.

3 Kyberhaktivismi on kasvanut merkittävästi. Kyberhyökkäyksillä pystytään nopeasti vastaamaan esimerkiksi lennokki-iskujen tai poliittisten päätösten jälkeen.

Näiden muutosten takia globaalisti tarkasteltuna kyberhyökkäysten määrä on lisääntynyt merkittävästi ja kohteena ovat entistä selkeämmin yhteiskuntien kaikkien kriittisimmät toiminnot. Hyökkäysmuotona ovat korostuneet kybersabotaasi, esimerkiksi ns. Wiper-hyökkäysten muodossa. Kybervakoilu on entistä kiinteämpi osa valtiollista tiedustelu- ja vakoilutoimintaa ja näin se on globaalin politiikan väline. Uusia tietovuotoja ja kybervakoiluatapauksia tulee ilmi kiihtyvällä tahdilla. Luottamus digitaalisiin järjestelmiin horjuu. Datan suojaaminen ja luokittelu sekä innovatiiviset suojaustavat korostuvat.

USA:n uudessa kyberstrategiassa korostetaan, hyökkäyksellisten toiminen merkitystä niin valtiollisten kybertoimijoiden kuin kyberrikollisten kapasiteetin ns. kybervoiman heikentämiseksi. Pelkkä suojautuminen ja passiivinen kyberpuolustus ei enää riitä. Tämä näkyy myös Naton kyberstrategisessa ajattelussa. Jäsenmailta edellytetään selkeämpää ja aktiivisempaa kyberdoktriinia. Jako sotilaallisen kyberturvallisuuden ja siviiliyhteiskunnan välillä hämärtyy entisestään.

Muutoksessa on aina myös mahdollisuus. Kybervoima on suhteellisen halpaa ja myös pienempien maiden ulottuvissa ja siten kyberturvallisuusyrityksille suuri mahdollisuus. Tulevaisuuden kyberturvallisuus perustuu uusin innovaatioihin ja osaamiseen – voittajia ovat ne, jotka oivaltavat ”älykkään kyberturvallisuuden” merkityksen. Tässä muutosprosessissa ei vanhat konstit ja toimintatapamallit yksin enää riitä. Parhaiten menestyvät ne maat ja yritykset, jotka panostavat uusiin kybersuorituskykyihin, joilla vastataan nopeasti muuttuvan kybermaailman muutokseen ja haasteisiin. On hyvä ymmärtää, että kybermaailma ei palaa entiseen ja muutosnopeus kasvaa. Globaali politiikka ohjaa entistä selkeämmin kybermaailman kehitystä. Strategista kybertilanneymmärrystä ja riskitietoisuutta tarvitaan toiminnan eri tasoilla, erityisesti kansallista turvallisuutta kehitettäessä.

AAPO CEDERBERG
Toimitusjohtaja ja perustaja,
Cyberwatch Finland

DIGITAALISTEN TAITOJEN PARANTAMISTA PAREMMAN EUROOPAN PUOLESTA

// Henna Virkkunen

Vuosi 2023 on Euroopan osaamisen teemavuosi. Digitaaliset taidot ovat tämän teemavuoden ytimessä. Digitaaliset perustaidot ovat laajalti käytössä jokapäiväisessä elämässämme, niin ammatillisessa kuin yksityisessäkin mielessä. Tällaisten taitojen käyttö muun muassa opiskelussa, työnteossa, tiedonhaussa, julkisten verkkopalvelujen käytössä ja yhteydenpidossa on usein välttämätöntä. Silti EU:n digitaalitalous- ja yhteiskuntaindeksin (DESI), eli Euroopan komission julkaiseman vuosiraportin, mukaan neljällä kymmenestä aikuisesta ja joka kolmannella Euroopassa työskentelevällä ei ole digitaalisia perustaitoja. Lisäksi naisten edustus on alhainen, sillä vain joka kuudes ICT-asiantuntija on nainen. Euroopan komissio on asettanut tavoitteeksi, että 70 prosentilla eurooppalaisista aikuisista on digitaaliset perustaidot vuoteen 2025 mennessä. EU:n digitaalisen vuosikymmenen tavoitteena on vastaavasti, että 80 prosentilla EU:n väestöstä olisi vähintään digitaaliset perustaidot vuoteen 2030 mennessä. Digitaalisten taitojen puute jättää väistämättä osan väestöstä digitaalisten palveluiden ulottumattomiin ja voi altistaa uudenlaisille uhille. Lisäksi digitaaliset taidot ovat avain onnistuneeseen vihreään ja digitaaliseen siirtymään.

Digitaalisten ja kyberturvallisuustaitojen vahvistaminen on tällä hetkellä keskeinen teema Euroopassa. Suomen tulisi käyttää tämä tilaisuus hyväksi, sillä tarjoamme runsaasti erilaisia koulutus- ja harjoitusmahdollisuuksia sekä kyberturvallisuuteen että digitaalisiin taitoihin liittyen. Suomi sijoittuikin DESI-indeksissä ensimmäiseksi vuonna 2022. Suomi onkin yksi johtavista EU-maista digitalisaation kehittämisessä. Esimerkiksi monet julkiset palvelut tarjotaan Suomessa verkkopalveluina. Suomi on EU-maiden kärjessä myös inhimillisen pääoman mittareilla mitattuna, ja on jo saavuttanut digitaalisen vuosikymmenen tavoitteen, jonka mukaan 80 prosentilla väestöstä on vähintään digitaaliset perustaidot. Digitaalisten taitojen välinen kuilu on kuitenkin edelleen laaja. Töitä on vielä tehtävänä, erityisesti ICT-asiantuntijoiden työllistymisen ja ICT-tutkinnon suorittaneiden osuuden lisäämisessä.

Vastauksena tähän haasteeseen Euroopan komissio esitteli kaksi neuvoston suositusta, jotka ovat EU:n jäsenvaltioille suunnattuja ei-sitovia säädöksiä, joiden tarkoituksena on tukea jäsenvaltioiden koulutussektoreita, jotta ne voisivat tarjota laadukasta digitaitojen koulutusta.

Neuvoston suositus menestyksekkään digitaalisen koulutuksen ja harjoittelun keskeisistä tekijöistä vaatii EU:n jäsenvaltioita takaamaan laadukkaan digitaalisen koulutuksen saatavuuden digitaalisen kuilun kaventamiseksi. Suositus luo puitteet investoinneille, hallinnolle ja opettajien koulutukselle, tavoitteena osallistava digitaalinen koulutus. Se edistää kokonaisvaltaista lähestymistapaa digitaaliseen koulutukseen ja laajempaa yhteistyötä sidosryhmien, mukaan lukien yksityisen sektorin, kanssa.

Neuvoston suositus digitaalisten taitojen parantamisesta koulutuksessa koskee kaikkia koulutustasoja. Suosituksessa korostetaan, että EU:n jäsenvaltioiden olisi tarjottava digitaitoja koskevaa koulutusta varhaisesta koulutusvaiheesta alkaen kaikilla koulutustasoilla kumulatiivisten tavoitteiden ja kohdennettujen toimien avulla myös tietyille vaikeasti tavoitettavissa oleville ryhmille. Jäsenvaltioiden olisi tuettava

aikuisten digitaalisten taitojen kehittämistä ja otettava käyttöön strategioita tietotekniikan alalla esiintyvien puutteiden poistamiseksi.

Digitaalisten taitojen parantamisen lisäksi Eurooppa tarvitsee kipeästi tietoa ja asiantuntemusta kyberturvallisuuden alalla. EU:lla on pula kyberturvallisuuden ammattilaisista. Vuonna 2022 kyberturvallisuustyövoiman tarve EU:ssa oli arviolta 883 000 asiantuntijaa. Samaan aikaan kyberturvallisuuden ammattilaisten pula EU:ssa vaihteli 260 000 ja 500 000 välillä. Ammattitaitoisia kyberturvallisuuden asiantuntijoita tarvitaan korkean tason kyberturvallisuuden saavuttamiseksi, mikä on välttämätöntä lisääntyneiden kyberhyökkäysten torjunnassa ja uusien uhkakuvien muodostamisessa. Tämä kasvattaa resilienssiä ja parantaa Euroopan asemaa kasvun ja kilpailukyvyn suhteen.

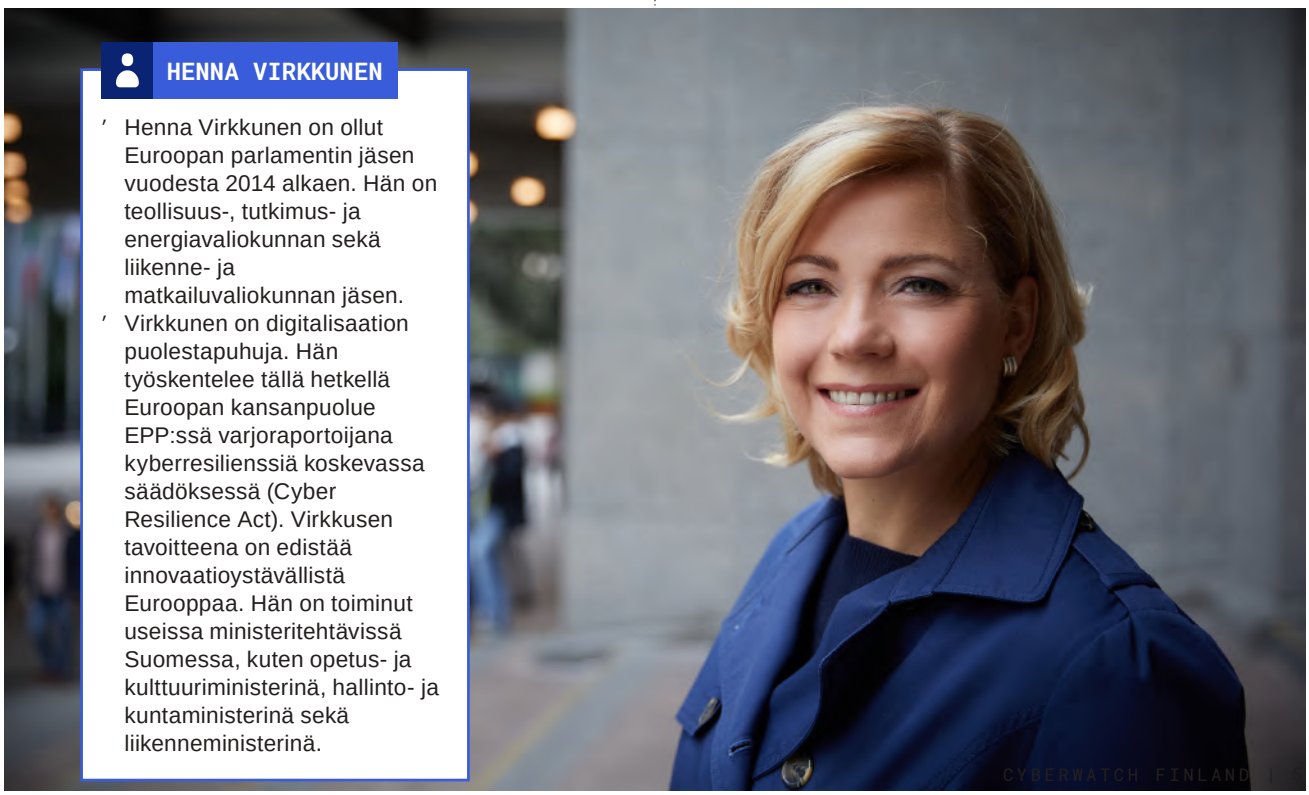
Tätä tarkoitusta varten Euroopan komissio hyväksyi tiedonannon kyberturvallisuuden osaamisakatemiasta (eng. Cybersecurity Skills Academyn) osana Euroopan osaamisen teemavuotta. Kyberturvallisuuden osaamisakatemian tavoitteena on kuroa umpeen kyberturvallisuuden osaamisvaje keskittämällä olemassa olevia aloitteita kyberosaamiseen ja parantamalla niiden koordinointia. Osaamisakatemia kokoaa Euroopasta ja kansallisilta tasoilta sekä julkiselta että yksityiseltä puolelta kootut koulutukset ja harjoitukset yhteen alustaan tiedon jakamisen helpottamiseksi.

Paras tapa taistella kehittyvää kyberturvallisuusuhkaa vastaan ja vastata uusiin uhkakuviin, on parantaa osaamista ja tietoisuutta sekä kehittää parempia kyberturvallisuustaitoja. Kaikki tämä edistää kestävämpää ja kilpailukykyisempää Eurooppaa. Korkeampi kyberturvallisuusvalmiuden taso koskee kaikkia yhteiskunnan sektoreita ja kaikkia sen kansalaisia, ei pelkästään alalla työskenteleviä asiantuntijoita.

Nämä uudet aloitteet ovat erittäin tervetulleita, mutta niitä on kaivattu jo pitkään. Niiden tavoitteet eivät ole vallankumouksellisia: Euroopan on kehitettävä pitkällä aikavälillä tehokas digitaalinen ekosysteemi, taattava digitaalisen koulutuksen yleinen saatavuus ja kehitettävä osallistava ja laadukas ekosysteemi, joka auttaa poistamaan digitaalista kuilua. Investointeja digitaaliseen infrastruktuuriin ja digitaalisiin laitteisiin tarvitaan.

Lisäksi olisi parannettava täydennyskoulutusten tunnustamista ja alan sertifioimien taitojen validointia, jotka jäävät perinteisten oppilaitosten ulkopuolelle. Tätä varten tuleva eurooppalainen digitaalisten taitojen sertifikaatti on hyödyllinen työkalu. On korostettava, ettei yksikään toimija voi ratkaista osaamisvajetta yksin. Julkisen ja yksityisen sektorin keskinäistä yhteistyötä olisi vahvistettava. Euroopan elinkeinoelämässä erityisesti pienillä ja keskisuurilla yrityksillä, on suuri potentiaali kehittää ratkaisuja osaamisvajeen ja digitaalisen kuilun poistamiseksi. Lisäksi digitaalisten taitojen parantaminen ei koske vain koulutuksesta vastaavaa hallinnollista sektoria, vaan se koskee laajan yhteiskunnallisen vaikutuksensa vuoksi kaikkia julkishallinnon sektoreita. Siksi yhtenäinen, koko hallinnon kattava lähestymistapa on tehokkain.

Uusi teknologia tuo mukanaan lukuisia mahdollisuuksia. Uuden teknologian käyttöönottoa ei voi hallita, mutta digitaalista osaamista voidaan kehittää teknologian ymmärtämiseksi ja hallitsemiseksi. Kyberturvallisuus ja digitaaliset taidot koskettavat kaikkia. Uudelleenkoulouttautumiseen, olemassa olevien taitojen kehittämiseen sekä jatkuvaan, elinikäiseen oppimiseen olisi kannustettava. ■



HENNA VIRKKUNEN

- Henna Virkkunen on ollut Euroopan parlamentin jäsen vuodesta 2014 alkaen. Hän on teollisuus-, tutkimus- ja energiavaliokunnan sekä liikenne- ja matkailuvaliokunnan jäsen.
- Virkkunen on digitalisaation puolestapuhuja. Hän työskentelee tällä hetkellä Euroopan kansanpuolue EPP:ssä varjoraportoijana kyberresilienssiä koskevassa säädöksessä (Cyber Resilience Act). Virkkusen tavoitteena on edistää innovaatioystävällistä Eurooppaa. Hän on toiminut useissa ministeritehtävissä Suomessa, kuten opetus- ja kulttuuriministerinä, hallinto- ja kuntaministerinä sekä liikenneministerinä.

VERKON PIMEÄ PUOLI

// Mira Stenhammar

Ihmiset käyttävät internettiä yhä enemmän kokoontuakseen yhteen ja ollakseen vuorovaikutuksessa muiden kanssa erilaisissa online-ympäristöissä ja sosiaalisen median alustoilla. Informaatio sosiaalisessa mediassa on dynaamista vuoropuhelua yksilöiden, yhteisöjen ja eturyhmien välillä ja niiden sisällä. Tieto ei ole pysyvää, vaan muuttuvaa ja suhteellista niiden merkitysantojen mukaan, joita ihmiset vuorovaikutustilanteissa tiedolle antavat. Sosiaalinen media ja verkkokeskustelujen kommentit ja kommenttien kommentit luovat nopeasti informaatiotilan, jossa erilaiset huhut, asenteet, tunteet ja tosiasiat rihmastoituvat niin, että faktojen tarkistaminen on lähes mahdotonta. Disinformaatiosta ja propagandasta on tullut sosiaalisessa mediassa yhä kehittyneempää ja vaikeammin jäljitettävää. Kunnianloukkaukset, uhkakuvien lietsonta ja väkivaltauhkaukset lisäävät samanlaisia negatiivisia tunteita kanavoivaa viestintää, jonka lopputuloksena voi olla kohonnut turvattomuuden tunne.

Internet tarjoaakin käyttäjilleen ainutlaatuisen ympäristön, jolle ei ole vertaista offline-maailmassa. Tietoverkkovälitteinen viestintä tarjoaa nopean, halvan ja anonyymin viestintävälineen monenlaisille ideologisille ääriryhmille ja internettiä usein käytetään vihan ja väkivallan lietsomiseen. Internetissä yksilö voi edustaa monia persoonallisuutensa tai identiteettinsä osa-alueita riippuen siitä, missä onlineryhmässä hän kulloinkin esiintyy.

INTERNET JA SOSIAALISET RYHMÄT

Jotta voidaan ymmärtää ihmisten välisiä eroavaisuuksia, täytyy ymmärtää yksilöiden käyttäytymisen taustalla olevia psykologisia mekanismeja, jotka vaikuttavat yksilöiden online-käyttäytymiseen. Internetin välityksellä tapahtuvan vuorovaikutuksen kasvokkain tapahtuvasta vuorovaikutuksesta erottaa neljä tekijää: suurempi anonymiteetti, fyysisten piirteiden merkityksen väheneminen, ajan parempi hallinta sekä samanmielisten löytämisen helppous. Erityisesti nuoret viettävät internetissä paljon aikaa usein etsiäkseen samanhenkisiä ystäviä ja ihmisiä. Kun he sitten löytävät tällaisia polarisoituneita ryhmiä vahvistaakseen omaa identiteettiään, voi se aiheuttaa sosiaalista kuplautumista, kognitiivista vääristymistä ja lisätä mustavalkoista maailmankuvaa. Yhä useammat nuoret myös altistuvat haitalliselle materiaalille, kuten epäasialliselle kielenkäytölle, väkivaltaiselle sisällölle, huumeille ja radikalisoituneille ryhmille.

Yksi tehokkaimmista tavoista, joilla ryhmät voivat yksilöön vaikuttaa, on normien vahvistaminen. Normit ovat ryhmän jäsenten yhteisiä käyttäytymisstandardeja. Kun ne on opittu, niitä noudatetaan sosiaalisen hyväksynnän saamiseksi. Ryhmiin kuuluminen usein myös muokkaa käyttäytymistämme. Yksilöt suhtautuvat myönteisemmin sisäryhmän jäseniin ja negatiivisesti ulkoryhmän jäseniin. Omaan ryhmään kuulumista saatetaan vahvistaa sillä, että muodostetaan negatiivisia assosiaatioita ulkoryhmän jäsenistä. Tämänkaltainen käyttäytyminen voi taas herättää vihamielisyyttä eri verkkoryhmien jäsenten välillä ja ryhmien sisällä.

PINTAVERKOSTA PIMEÄÄN VERKKOON

Aggressiivinen käyttäytyminen internetissä on monellakin tavoin helppoa. Internettiin ja keskustelufoorumeille pääsy on mahdollista käytännössä koska vaan, eikä sitä kukaan pysty erityisemmin rajoittamaan. Samoin verkon sisältö on monelta osin sääntelemätöntä ja kommunikointia voidaan käydä anonyymisti. Anonyymiys viittaa nimettömänä tai yksityisenä toimimiseen. Yksityisyyttä on usein perusteltu yksilöiden perustavanlaatuisena ihmisoikeutena ja tarpeena omaan henkilökohtaiseen tilaan. Ihmisillä tulisi olla vapaus saada olla tekemisissä toisten kanssa ilman valvontaa. Anonyymit järjestelmät mah-

dollistavat sen, että henkilöstä ei löydy tietoa ilman hänen omaa tahtoansa. Anonyymiydellä on kuitenkin kaksi puolta: yhtäältä sillä suojellaan tietojen yksityisyyttä, kun taas toisaalta sillä minimoidaan oman toiminnan vastuullisuus. Anonyymina kommunikointi luo vääristynyttä mielikuvaa siitä, ettei omista sanomisista tarvitse ottaa vastuuta. Muut verkkokeskustelijat voivat osaltaan tukea ja kannustaa anonyymiin vihamieliseen käyttäytymiseen. Verkossa on ”helppo” hyökätä muita anonyymeja ja pseudonyymeja vastaan, koska he ovat tuntemattomia ja tämän vuoksi epäinhimillisempiä, eikä kostoa tarvitse pelätä.

Niiden henkilöiden ja ryhmien vuorovaikutusta, joiden keskusteluja ja kommunikointia leimaavat viha ja negatiivisuus, voi olla vaikea toteuttaa pintaverkon puolella. Ne ihmiset, joiden mielipiteitä pyritään pintaverkon puolella moderoimaan ja sensuroimaan, päätyvätkin helpommin pimeän verkon puolelle tuomaan esille mielipiteitään. Sosiaalisesta mediasta ja etenkin pimeästä verkosta on tullut yhä enemmän rikollisuuden, väärinkäytön ja vihapuheen foorumi, koska käyttäjien luoman sisällön suodattamiseen ei ole olemassa selkeitä ohjausmekanismeja. Sosiaalisen median pimeän puolen voidaan ajatella olevan kokoelma negatiivisia ilmiötä, jotka liittyvät informaatioteknologian käyttöön ja jotka voivat vaikuttaa yksilöiden, organisaatioiden ja yhteiskuntien hyvinvointiin. Sosiaalisen median pimeä puoli voi muodostaa todellisen uhan kansalliselle turvallisuudelle, koska tulevat sukupolvet syntyvät erilaisten polarisoituneiden online-tietoverkkojen ympäristöön.

ALUSTA KYBERRIKOLLISUUDEN KEHITTYMISELLE

Etenkin pimeä verkko on monella tapaa ihanteellinen areena monenlaisille rikollisille ja ideologisille ääriryhmille, koska toimintaa siellä on vaikea minkään yksittäisen tahon tai valtion puolesta säädellä ja se tarjoaa anonyymin multimediaympäristön kaikkine palveluineen. Kyberrikollisryhmiä voidaan tarkastella niiden ryhmäidentiteetin perusteella sekä toimintaa ohjaavan motiivin perusteella. Ryhmät voivat olla tiukasti ohjattuja tai vaihtoehtoisesti ilman hierarkkista rakennetta. Kyberrikollisryhmistä voidaan tunnistaa kolme keskeistä rikollisryhmää:

1) perinteiset rikollisryhmät,
2) järjestäytyneet kyberrikollisryhmät sekä
3) ideologisesti ja poliittisesti motivoituneet kyberrikollisryhmät.

Usein näillä ryhmillä on järjestäytynyttä toimintaa myös? verkkoympäristön ulkopuolella. Haktivistit ja poliittisesti motivoituneet hakkeriryhmät ovat myös yksi uusin kyberrikollisryhmän muoto. Edellä mainittujen ryhmien lisäksi ei pidä unohtaa yksilöitä, jotka yhä enemmässä määrin käyttävät teknologiaa laittomiin tarkoituksiin ja epäasialliseen toimintaan.

Yksi merkittävin tekijä kyberrikollisuuden kasvuun on ollut tarvittavien työkalujen helppo saatavuus. Kehittyneiden teknologioiden ja menetelmien saatavuus tietoverkkorikosten tekemiseen on kasvanut huomattavasti ja niitä on saatavilla verraten helposti pimeästä verkosta. Tämä kehitys on mahdollistanut monia teknologiaa vähemmän osaavia suorittamaan hyvinkin edistyneitä kyberrikoksia. Samoin sosiaalisen median alustat mahdollistavat matalalla kynnyksellä toisten kiusaamisen, häirinnän ja uhkailun. Teknologia vähentää myös yksilön kiinnijäämisen riskejä, sillä erilaisen rikollisuuden havaitseminen ja tuomitseminen on online-ympäristössä paljon haastavampaa kuin offline-ympäristössä. Kyberavaruudessa on myös helppo maksimoida rikoksella saatu tuotto ottamalla kohteeksi useita uhreja samanaikaisesti.

Myös erilaiset poliittiset ja yhteiskunnalliset liikkeet käyttävät teknologiaa levittääkseen tietoa aatteistaan ja koordinoidakseen toimintaa sekä verkossa että sen ulkopuolella. Internetistä on tullut kriittinen työkalu erilaisille ääri- ja terroristiryhmille ideologioiden levittämiseksi ja yksilöiden radikalisoimiseksi väkivaltaan. Ääriryhmät ja ideologiset hakkerit ovat löytäneet tapoja käyttää internettiä mekanismina hyökätäkseen hallintoa ja valtaapitäviä vastaan eri puolilla maailmaa. Tällä tavoin teknologia on muun muassa laajentanut ääriryhmien kykyä vaikuttaa populaatioihin ja kohteisiin paljon enemmän, mitä fyysisessä maailmassa.

YHTEENVETO

Pimeä verkko eli darkweb on eräänlainen piilo-organisaatio, joka yhdistää perinteiset laittomat toimijat ja hakkerit anonyymin kyberinfrastruktuurin kautta. Pimeä verkko on viimeisen vuosien ajan kehittynyt vuorovaikutusvälineenä, mikä on entistään lisännyt siellä tapahtuvaa epäasiallista toimintaa ja kyberrikollisuutta. Pimeä verkko on sekoitus rikollisuutta ja idealismia ja kaikkea niiden väliltä. Sen olemassaolo onkin monitahoinen ja monelta osin problemaattinen asia. Vaikka pimeä verkko on myös vapaan ilmaisun paikka toisinajattelijoille, sananvapauden puolustajille ja ilmiantajille, on se mahdollistanut myös monenlaiset uudet rikollisuuden muodot ja helpottanut rikosten tekemistä. Tästä syystä pimeän verkon käyttö luo eräänlaista stigmaa sen käyttäjilleen. Pimeässä verkossa rehottava rikollisuus ja sen jäljittämisen haasteet ovat omiaan lisäämään yhteiskunnissa koettua turvattomuuden tunnetta. ■

MIRA STENHAMMAR

Johtava kyberanalyytikko, Cyberwatch Finland

UKRAINAN SOTA EI RATKEA KYBERTAISTELUISSA

// Markus Vaija

Ukrainan sota on ensimmäinen konflikti maailmassa, jossa kyberympäristö näyttelee merkittävää roolia yhtenä sodan taistelukentistä. Perinteisesti näitä kenttiä on ajateltu olevan maa, meri, ilma ja joskus myös avaruus. Ukrainassa on nyt ensimmäistä kertaa saatu nähdä, minkälainen rooli kybermaailman taistelukentällä on laajamittaisessa, valtioiden välisessä sodassa. Kyseessä ei kuitenkaan ole ensimmäinen valtioiden välinen konflikti, jossa kyberympäristöä on hyödynnetty laajasti. Eri puolin maailmaa on jo vuosia käyty, ja käydään jatkuvasti, valtioiden välisiä kamppailuja kyberympäristössä. Ukrainan sota on (toistaiseksi) kuitenkin ainoa merkittävä konflikti, jossa käynnissä on kineettisen sodan kanssa samaan aikaan myös kybersota. Juuri tästä perspektiivistä sitä onkin mielenkiintoista tarkastella ja pyrkiä hahmottamaan mikä rooli kyberoperaatioilla on ollut sodan kokonaiskuvan kannalta.

Ennen sodan alkua oli olemassa ajatuksia ja teorioita siitä, miten kyberoperaatioita voitaisiin hyödyntää muun sotatoiminnan tukena. Käytäntö on kuitenkin osoittanut, että monet näistä käsityksistä ovat olleet vääriä. Nyt tarkasteltaessa tulisikin pyrkiä ymmärtämään miten kyberoperaatiota on todellisuudessa onnistuttu hyödyntämään laajempien strategisten tavoitteiden edistämiseksi, minkälainen niiden vaikutus on ollut ja miten kybertoiminta on vaikuttanut muiden taistelukenttien operaatioihin. Käynnissä olevaa sotaa on kuitenkin äärimmäisen vaikea tarkastella paitsi epäluotettavan tai värittyneen tiedon vuoksi, mutta myös koska molemmat osapuolet pyrkivät aktiivisesti salaamaan niille epäedullisen tai luonteeltaan kriittisen tiedon. Tämän vuoksi etenkin operaatioiden vaikuttavuutta on lähes mahdotonta arvioida. Vaikka yksittäisiä tapauksia löytyykin esimerkiksi siitä, miten Ukraina on hyödyntänyt kybertiedustelua venäläisten upseerien tai tukikohtien sijainnin selvittämiseksi, on näkyvissä todennäköisesti vain jäävuoren huippu. Kyberympäristön taisteluiden seuraamisen tekee vielä hankalammaksi se, että suurin osa operaatioista tapahtuu julkisen silmän ulottumattomissa ja kaikessa hiljaisuudessa, ilman massiivisia reportaaseja. Parhaat johtopäätökset Ukrainan sodasta ja sen kyberkomponentista voidaankin tehdä todennäköisesti vasta vuosien päästä. On kuitenkin mahdollista varovaisesti arvioida, mitä julkisesti saatavilla olevan tiedon perusteella voidaan sanoa kyberoperaatioista osana laajempaa konfliktia, vaikka niiden painoarvon mittaaminen koko sodan kannalta on vielä vaikeaa.

Sodan alkaessa kybersodasta tuntui olevan vallalla kaksi käsitystä, joista molemmat ovat myöhemmin osoittautuneet virheelliseksi. Ensinnäkin Venäjän oletettiin olevan kybersuorituskyvyltään ylivoimainen suhteessa Ukrainaan. Tämän lisäksi sen ollessa hyökkäävässä, ja siten paremmassa asemassa aloitteen tekemisen edun myötä, odotettiin, että se melko nopeasti saavuttaa merkittävän kybermaailman voiton ja lamauttaa Ukrainan tietojärjestelmät. Toiseksi tunnuttiin odottavan merkittävää yksittäistä kyberhyökkäystä tai -iskua, jonka vaikutukset suuntaan tai toiseen olisivat olleet selkeitä ja merkittäviä. Vaikka merkittäviä kyberoperaatioita molemmin puolin on kyllä nähty, ei monellakaan näistä voida sanoa olleen laajoja, useita päiviä tai viikkoja kestäneitä vaikutuksia. Kyberympäristössä käytävä mittelö on osoittautunut tasaväkiseksi ja hitaaksi kulutussodaksi, jossa molemmat osapuolet todennäköisesti yhä pohtivat parasta tapaa hyödyntää sitä laajempien strategisten tavoitteiden saavuttamiseksi.

Ennusteista poikkeavan kehityskulun syyksi pantiin sodan muutaman ensimmäisen kuukauden jälkeen pitkälti väärät arviot voimasuhteista; ei niinkään kokonaisvaltaisesti väärä käsitys kybersodan luonteesta. Syitä siihen, miksi merkittävää kybermaailman voittoa ei tapahtunut, ajateltiin olevan sekä yliarviot Venäjän suorituskyvystä että ennakoimaton länsimaiden tuki Ukrainalle. Vaikka edellä mainitut seikat ovat varmasti vaikuttaneet siihen, miksi odotukset eivät toteutuneet, on pikkuhiljaa tultu siihen tulokseen, että kyberympäristön mahdollisuudet sodassa ymmärrettiin alun perinkin väärin. Sodassa ei ole tapahtunut, eikä myöskään tule tapahtumaan, merkittävää kyberympäristön ratkaisutaistelua, sillä sellainen ei taistelukentän luonteen takia yksinkertaisesti ole mahdollista tai ainakaan kovin todennäköistä.

Tämä mielipide uudesta kybersodan kuvasta vaikuttaa etenkin Yhdysvalloissa saaneen jalansijaa. Viime kuussa yhdysvaltalainen ajatushautomo Atlantic Council järjesti Melding cyber and kinetic in conflict paneelikeskustelun, jossa asiantuntijat sekä asevoimista että yliopistomaailmasta pyrkivät viimeisen vuoden oppien valossa uudelleen määrittelemään sen, miten kyberoperaatiot tulisi ymmärtää laajemmassa sodan kontekstissa. Paneelin mukaan Ukrainan sodan tapahtumia tarkasteltaessa aiempi ymmärrys kyberympäristön roolista on todellakin ollut väärä ja, jotta hyödyllisiä oppeja voidaan tulevaisuuden konfliktien varalle saada, käsitystä kybermaailmasta sodan kenttänä tulisi muuttaa. Atlantic Councilin kyberoperaatioiden asiantuntija Michael Martelle kuvasi, että ennen sotaa moni tuntui odottavan kybermaailmassa tapahtuvaa merkittävää ratkaisutaistelua, eräänlaista kybermaailman Pearl Harboria. Ennakko-oletus oli, että sodassa tapahtuu toisen maailmansodan käännekohdan kaltainen yksittäinen, koko sodan kuvaa muokkaava taistelu. Tämä lähestymistapa on hänen mukaansa väärä. Kyberoperaatioita pitäisikin verrata Pearl Harborin sijaan saman sodan myöhäisempään ja selkeästi vähemmän mediaseksikkäämpään Tyynen valtameren sukellusvenekampanjaan. Tässä pitkään jatkuneessa operaatiossa Yhdysvaltojen sukellusveneet toimivat kaikessa hiljaisuudessa ja poissa julkisesta tietoisuudesta, mutta kuluttivat hiljalleen Japanin sotakoneistoa heikentämällä etenkin sen huoltokykyä ja tuottamalla merkittävää tiedustelutietoa ilman yksittäisiä suuria voitettuja taisteluja.

Kyberympäristössä käytävä mittelö on osoittautunut tasaväkiseksi ja hitaaksi kulutussodaksi, jossa molemmat osapuolet todennäköisesti yhä pohtivat parasta tapaa hyödyntää sitä laajempien strategisten tavoitteiden saavuttamiseksi.

Sukellusveneanalogiaa puoltaa se, että siinä kybertoimintaympäristön operaatioita verrataan näkymättömään ja aikansa korkeinta teknologiaa hyödyntävään toimintaan. Toisaalta ainakaan tähän mennessä kyberaseilla, toisin kuin sukellusveneillä, ei ole suoranaisesti ammuttu tai tuhottu mitään, vaan kyse on häirinnästä, hetkellistä toimintakatkoksista tai tiedon hankinnasta. Toinen mahdollinen vertaus toisesta maailmansodasta löytyisi strategisista pommikonekampanjoista, joilla niin ikään tarkoituksena oli heikentää vastapuolen logistiikkaa tai huoltokykyä. Samoin kuin pommituksilla, kyberiskuilla on ollut merkittävä vaikutus myös siviiliväestön olosuhteisiin sodan keskellä ja siihen, miten paljon sota näkyy ja tuntuu heidän elämässään. Kyberoperaatioilla on myös ollut merkittävä propaganda-arvo ja molemmat sodan osapuolet ovat käyttäneet onnistuneita iskujaan tehokkaasti strategisen viestinnän työkaluina.

Kyberympäristö on myös mahdollistanut täysin uudenlaisen tavan osallistaa sekä omia kansalaisia että ulkomailta tulevaa apua sotaponnisteluihin. Ukrainan sodassa molemmat osapuolet ovat hyödyntäneet joukkoistamista kyberoperaatioissaan. Joukkoistaminen ja sen hyödyt ovat näkyneet niin ulkomaisia kyberosaajia rekrytoivan Ukrainan IT-armeijan toiminnassa, Venäjän hyödyntämien isänmaallisten kyberrikollisisten iskuissa kuin ukrainalaisille siviileille suunnattujen mobiilisovellusten käytössä. Näillä applikaatioilla ukrainan kansalaiset ovat voineet ilmoittaa havaitsemistaan venäläisistä ilma-aluksista tai muusta sotilastoiminnasta nopeasti ja suoraan asevoimille. Joukkoistamisen vaikutus on ollut sekä konkreettinen tuki operaatioille, mutta etenkin Ukrainan siviiliväestön kohdalla sillä on varmasti ollut kriisinsietokykyä parantava vaikutus. Kun yksittäiset kansalaiset voivat konkreettisesti kokea olevansa hyödyllinen osa konfliktia ja auttavansa maataan sodan keskellä, on tällä positiivinen vaikutus myös kriisinsietokykyyn, vaikka toiminnan todelliset vaikutukset muuten jäisivät vaatimattomiksi.

Kyberympäristö kommunikaation ja informaatiovaikuttamisen työkaluna on myös muuttanut paljon perinteistä sotatoimiympäristöä. Ukraina onnistui heti sodan alkuhetkiltä alkaen saamaan laajan kansainvälisen tuen ja sympatian puolelleen. Merkittävässä roolissa tässä olivat sekä toimivat tietoliikenneyhteydet että mahdollisuus viestiä suoraan konfliktialueelta. Viestinvälityksen nopeus ja mahdollisuus seurata sodan tapahtumia lähes reaaliajassa mistä päin maailmaa tahansa, on vaikuttanut voimakkaasti siihen, miten paljon huomiota Ukrainan konflikti on saanut ja siten myös ulkomailta tulleen tuen määrään.

Tulee kuitenkin muistaa, että todellista kuvaa siitä, mitä kaikkea kyberoperaatioilla on onnistuttu saavuttamaan ja miten tehokkaasti niillä on onnistuttu tukemaan esimerkiksi tiedustelua, on yksinkertaisesti mahdotonta tietää tässä vaiheessa. Arvioitaessa kyberympäristön osuutta sodassa, on hyvä pitää mielessä, että Ukrainan sota on tässä suhteessa nimenomaan ensimmäinen, ja kenties jonkinlaisena koenäyttämönä toimiva konflikti. On mahdollista, että tulevaisuudessa kyberoperaatioiden merkitys ja käyttö osana sotatoimia poikkeaa huomattavasti siitä, mitä nyt on saatu nähdä. Historiasta voidaan etsiä lisää analogiaa: ilmasodankäynti, joka ensimmäisen maailmansodan aikana vasta teki nousua merkittäväksi taistelukentäksi, oli vain muutamaa vuosikymmentä myöhemmin luonteeltaan täysin erilainen, huomattavasti kehittynyt, ja hyvin keskeisessä roolissa toisen maailmansodan aikaan. Ensimmäisessä maailmansodassa ilmasota oli varsin uusi käsite, jonka hyötyjä ja mahdollisuuksia vasta etsittiin ja kehiteltiin. Toisessa maailmansodassa se puolestaan oli jo konkreettinen ja varsin oleellinen osa strategista kamppailua ja sodan lopputulosta.

Vaikuttaa siis todennäköiseltä, että Ukrainan sotaa ei ratkaista kybermaailman taistelukentällä. Se on sodan kontekstissa uusi toimintaympäristö, jonka merkitystä selvästi yliarvioitiin ennen sodan alkua. Kyberoperaatiot eivät silti ole olleet turhia, tai kybermaailman rooli olematon. Niiden merkitys on vain osoittautunut vähäisemmäksi ja selvästi erilaiseksi kuin ennakkoon oletettiin. Kyse on kuitenkin varsin nopeasti kehittyvästä ja muuttuvasta toimintakentästä, ja toisin kuin ilmasodan kohdalla, ei varmastikaan tarvitse odottaa vuosikymmenten ajan, että kybersodan kuva jälleen muuttuu merkittävästi. ■

MARKUS VAIJA

Kyberanalyytikko,
Cyberwatch Finland

KYBERSOTA VENÄLÄISIN SILMIN

// Mikko Hynönen

Ukrainan sotaa on kutsuttu raflaavasti maailman ensimmäiseksi täyden mittakaavan kybersodaksi[1]. Voittajasta ei vielä ole tietoa, mutta iskuja on nähty puolin ja toisin. Venäjä on kohdistanut iskujaan esimerkiksi satelliitteja vastaan[2], targetoinut ukrainalaisia kalasteluviesteillä[3] sekä tehnyt laajoja palvelunestohyökkäyksiä Eurooppaan[4]. Vastaavasti Venäjä on itsekin kokenut kyberrintaman takaiskuja esimerkiksi kybersabotaasin[5] ja tietovuotojen merkeissä[6].

Tässä artikkelissa tarkastellaan kybersotaa yksittäisten operaatioiden sijaan laajemman ja hieman erilaisen linssin läpi. Artikkelissa pyritään kuvaamaan sodan kyberulottuvuuden merkitystä, hyötyjä ja haasteita Venäjän näkökulmasta. Havaittavissa on sekä Venäjän kannalta "positiivisia" asioita että ongelmallisia kehityskulkuja. Venäjälle kyberhyökkäykset vaikuttavat toimivan eräänlaisena epävirallisena ulkopolitiikan jatkeena, minkä lisäksi pyrkimys käyttää kyberrintamaa kansaa ja vapaaehtoisia aktivoivana tekijänä, on merkittävää. Haasteita aiheuttaa oman kyberpuolustuksen epäonnistuminen sekä erityisesti osaajapula, jonka voidaan olettaa edelleen tulevaisuudessa kasvavan.

KYBERHYÖKKÄYSTEN MERKITYS VENÄJÄLLE

Kyberhyökkäysten merkitystä sodassa ei tule liikaa korostaa, mutta ei myöskään väheksyä. Vaikuttaa siltä, että sota tullaan todennäköisesti ratkaisemaan fyysisellä taistelukentällä, perinteisen sodankäynnin keinoin, mutta kyberoperaatioilla on tässä tietysti vähintäänkin fyysisiä operaatioita tukeva rooli. Kyberhyökkäysten vaikutukset ovat moninaisia: ne rapauttavat sekä vastustajan joukkojen että siviiliväestön moraalia, sitovat vastustajan resursseja sekä toimivat taistelukentällä operaatioiden tukena. Asiantuntija-arvioissa on kuitenkin arvioitu, että Venäjä ei ole onnistunut konventionaalisen- ja kybersodankäynnin yhdistämisessä, saati saavuttanut kyberoperaatioilla strategisia vaikutuksia[7]. Tämä ei tarkoita sitä, etteikö Venäjä kerryttäisi hyödyllistä oppia tulevaisuutta ajatellen ja onnistuisi vastaisuudessa kehittämään toimintaansa. Joidenkin arvioiden mukaan kehitystä onkin sodan aikana tapahtunut, jos viime aikojen operaatioita verrataan sodan alun iskuihin[8].

Kyberoperaatioiden laajempi merkitys ei Venäjän tapauksessa muodostu pelkästä vastustajalle aiheutetusta tuhosta ja haitasta, sillä toiminnalle on lueteltavissa myös lukemattomia muita hyötyjä. Yksinkertaistetun sotilaallisen linssin lisäksi kyberoperaatioita on mielekästä tarkastella osana Venäjän ulko- ja sisäpolitiikkaa. Carl Von Clausewitzin klassista ”sota on politiikan jatkamista toisin keinoin” -sitaattia mukaillen, Venäjän kyberhyökkäykset ovat ulkopolitiikan jatkamista toisin keinoin. Tämä pätee etenkin Ukrainan ulkopuolelle kohdistettuihin kyberhyökkäyksiin. On tunnustettu tosiasia, että Venäjällä rajat rikollisten hakkeriryhmien ja valtion välillä ovat häilyvät[9]. Venäjällä onkin käytettävissään sekä valtion toiminnasta irralliset, tai löyhässä lieassa olevat, rikollisjengit, mutta myös suoraan kontrollissa olevia tiedustelupalvelujen alaisia APT-ryhmiä. Näin ollen lähes kaiken venäläistaustaisten kybertoiminnan tekojen taustalla on todennäköisesti jossain määrin valtion ohjaava käsi. Kyberhyökkäysten voidaankin tulkita lähettävän strateginen viesti pelkän kiusanteon tai sotilaallisten tavoitteiden sijaan. Esimerkiksi kevään aikana tammikuussa Saksaan ja toukokuun alussa Suomeen kohdistuneiden palvelunestohyökkäysten viesti oli selvä. Ensin mainittu ajoittui Leopard-panssarivaunujen luovutuspäätöksen yhteyteen, jälkimmäinen taas Suomen Nato-jäsenyyden varmistumiseen. Muiden keinojen puuttuessa tai niiden ohella, kyberhyökkäykset ovat keino osoittaa tyytymättömyyttä päätöksiin. Virallisesti Kreml on tietenkin kiistänyt hyökkäysten liittymiseen Venäjään ja kutsunut väitteitä muun muassa ”absurdeiksi”[10].

Kyberhyökkäyksille on annettavissa myös muita merkityksiä. Sotatoimien muuten takkuillessa, tiedot onnistuneista kyberhyökkäyksistä nostattavat kansakunnan moraalia ja voivat toimia propaganda-aseena. Valtaapitävien taholta onkin annettu suora moraalinen tuki myös valtiosta riippumattomien hakkerien toiminnalle, mistä kielii keväällä käyty keskustelu Venäjän etujen vuoksi toimivien hakkerien vapauttamisesta rikosvastuusta[11]. Tällä tavalla Venäjä antaa tavallisille kansalaisille mahdollisuuden osallistua sotaan ja isänmaan tukemiseen. Joukkoistaminen ei tietenkään ole pelkästään venäläinen ilmiö, sillä pitkin sotaa kybervapaaehtoiset ympäri maailman ovat kohdistaneet iskuja Venäjää vastaan. Länsimaissa tästä on kirjoitettu paljon, Suomessa niin YLE[12] kuin Helsingin Sanomat[13] tarttuivat aiheeseen ensimmäisenä sotakeväänä.

KYBERHYÖKKÄYKSET JA OSAAJAPULA VAIKEUTTAVAT VENÄJÄN ASEMAA

Vaikka venäläiset hakkeriryhmät kerskuvat Telegram-kanavillaan onnistuneista kyberiskuista ja hakkereiden toimintaa pyritään helpottamaan, on Venäjällä ollut vaikeuksia pitää oma pesänsä puhtaana. Venäjään on kohdistunut massiivinen määrä kyberhyökkäyksiä ja venäläisessä mediassa on ollut kasvavissa määrin uutisointia niistä. Esimerkiksi Izvestija-lehti on raportoinut vuoden 2023 ensimmäisellä kvartaalilla DDoS-hyökkäysten tuplaantuneen verrattuna vuoden takaiseen[14]. Samaisessa lehdessä on uutisoitu FSB:n lausunnosta, jonka mukaan USA ja Nato käyttävät Ukrainaa alustanaan kyberhyökkäyksiin[15]. Lisäksi viranomaiset ilmoittivat maaliskuussa, että yli 165 miljoonaa venäläisiä koskevaa henkilötietoa on vuotanut vuoden alun jälkeen[16].

Kyberturvan tasosta Venäjällä on vaikea saada kattavaa kuvaa. Esimerkiksi Kansainvälisen televiestintäliitto ITU:n (International Telecommunication Union) globaalissa kyberturvaindeksissä Venäjä saavutti viidennen sijan vuonna 2020[17]. Toisaalta uutisoinnit onnistuneista hyökkäyksistä ja vuotaneista tunnuksista puhuvat sijoitusta vastaan. Silmiin pistävää on, että vaikka häiriöistä ja tietovuodoista raportoidaan, ei niillä ole ollut suuria tai lamauttavia vaikutuksia, eivätkä ne ole hallinneet mediatilaa. Mahdollinen on myös tarkoituksenmukainen pyrkimys luoda kuva, että kyberhyökkäykset eivät ole tehokkaita. Kyynisemmän näkökulman mukaan valtio ei vain välitä kansalaistensa vuotaneista tiedoista. Esimerkiksi oppositiomedia Meduza on huomauttanut tietoturvasakkojen olleen yleensä merkittävissäkin vuodoissa vain 60 000–100 000 ruplan (noin 700–1200 €) välillä[18].

Valtiojohdon näkökulmasta länsimaisia hakkereita ja kansalaisten tietojen vuotamista huolestuttavamman uhan muodostaa kuitenkin sisältä käsin kumpuava vastarinta. Esimerkiksi valkovenäläisten hakkereiden tiedetään iskeneen rautatieinfrastruktuuria kohtaan, mikä on hidastanut toimitusten kuljettamista rintamalle[5]. Myös sisäpiiriuhka on realisoitunut, kun tiedustelupalveluihin liitännäisen Vulkan-yhtiön tiedostoja, kuten sisäisiä sähköposteja vuosi tyytymättömän työntekijän toimesta[6].

Monet myös äänestävät jaloillaan: oman haasteensa aiheuttaa ammattilaisten lähteminen ja siitä johtuva, kasvava osaajapula, jota sota on edelleen pahentanut. Tietotekniikan koulutusohjelmat Venäjällä ovat perinteisesti olleet laadukkaita ja maan yliopistojen joukkueet ovat vuosien ajan saavuttaneet menestystä yliopistojen välisissä koodauskilpailuissa[19]. Sodan myötä yrityksillä on ollut haasteita pitää kiinni työntekijöistään ja jopa sadantuhannen it-alan ammattilaisen uskotaan muuttaneen pois maasta[20]. Ongelmaan on pyritty ratkaisemaan parantamalla etätyömahdollisuuksia. Esimerkiksi it-jätti Yandex on avaamassa jo toisen toimiston Belgradiin, joka on suosittu kohde emigraatioille[21]. Valtio kuitenkin pyrkii suitsimaan maastamuuttoa. Viimeisimpänä duumassa on meneillään lakiuudistus, jolla pyritään nostamaan ulkomailta käsin venäläisille yhtiöille työskentelevien tietotyöläisten veroprosentin 13 %:sta jopa 30 %:iin[22]. Yritysten ja valtion välillä onkin havaittavissa kädenvääntöä, valtion käyttäessä keppiä ja porkkanaa it-osaajien saamiseksi takaisin Venäjälle, yritysten lisätessä vaihtoehtoja ulkomailla työskentelyyn. Osaajapula voi näkyä myös yllättävällä tavalla. Esimerkiksi koko kevään on puhuttu tekoälyn kehityksestä ChatGPT:n ja sen kilpailevien vaihtoehtojen myötä. Kysymykseksi voi nousta, kuka kehittää venäläistä tekoälyä tai uuden sukupolven kyberaseita, jos osaajat karkaavat pois maasta?

LÄHTEET:

1 https://www.atlanticcouncil.org/blogs/ukrainealert/vladimir-putins-ukraine-invasion-is-the-worlds-first-full-scale-cyberwar/
2 https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/
3 https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/
4 https://www.euronews.com/2023/01/26/russian-hackers-launch-cyberattack-on-germany-in-leopard-retaliation
5 https://meduza.io/en/feature/2022/07/05/the-guerrilla-war-on-belarus-s-railways
6 https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics
7 https://www.swp-berlin.org/10.18449/2023C23/
8 https://www.iiss.org/research-paper/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences
9 https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a
10 https://iz.ru/1459891/2023-01-25/peskov-nazval-absurdom-assotciatciiu-liubykh-khakerskikh-atak-s-rossiei
11 https://tass.ru/obschestvo/17021313
12 https://yle.fi/a/3-12338836
13 https://www.hs.fi/ulkomaat/art-2000008649170.html
14 https://iz.ru/1502326/mariia-frolova/poimali-volnu-chto-stoit-za-vesennimi-ddos-atakami-na-rossiiskie-kompanii
15 https://iz.ru/1497823/2023-04-13/fsb-soobshchilo-ob-uchastii-pentagona-v-kiberatakakh-protiv-rossii
16 https://tass.ru/obschestvo/17275519
17 https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
18 https://meduza.io/feature/2022/12/22/nikogda-esche-lichnye-dannye-rossiyan-ne-utekali-v-otkrytyy-dostup-tak-chasto-i-v-takom-ob-eme-kak-v-2022-m-odna-iz-prichin-voyna https://meduza.io/feature/2022/12/22/nikogda-esche-lichnye-dannye-rossiyan-ne-utekali-v-otkrytyy-dostup-tak-chasto-i-v-takom-ob-eme-kak-v-2022-m-odna-iz-prichin-voyna
19 https://icpc.global/worldfinals/fact-sheet/ICPC-Fact-Sheet.pdf
20 https://www.themoscowtimes.com/2022/12/20/moscow-says-100k-it-specialists-have-left-russia-this-year-a79754
21 https://www.forbes.ru/svoi-biznes/486667-andeks-otkroet-vtoroj-ofis-v-belgrade
22 http://duma.gov.ru/news/56961/

> **Sotatoimien muuten takkuillessa, tiedot onnistuneista kyberhyökkäyksistä nostattavat kansakunnan moraalia ja voivat toimia propaganda-aseena.**

JOHTOPÄÄTÖKSET:

Venäjän kannalta sodan kyberulottuvuuteen liittyy sekä uhkia että mahdollisuuksia. Kyberhyökkäykset toimivat sotatoimien tukena ja niiden avulla Venäjä kerryttää oppia tulevaisuuden operaatioitaan varten. Laajemman näkökulman mukaan kyberhyökkäykset lähettävät strategista viestiä ja toimivat epävirallisena ulkopolitiikan viestinvälittäjänä. Samalla kyberhyökkäykset ja niihin kannustaminen toimivat propagandan välineenä sekä sodan joukkoistamisen muotona.

Vaakakupin toisessa päässä Venäjä on itse joutunut ennennäkemättömän kyberhyökyaallon uhriksi. Tietoja vuotaa, mutta reagointi ei ainakaan toistaiseksi ole ollut näkyvää. Kyberulottuvuus muodostaa kasvavan uhkatekijän, jota sisäpiiriuhka tai yhä akuutimmaksi muodostuva osaajapula eivät vähennä. ■

MIKKO HYNÖNEN

Kyberanalyytikko,
Cyberwatch Finland

KYBERTURVALLISUUDEN OSA-ALUEET ENNEN JA NYT

// Jukka Lång, Johanna Tuohino and Julia Vikström

Nykyinen kyberturvallisuuskenttä on pakottanut meidät oppimaan selviytymään jatkuvasti ympäröivistä kyberuhkista. Avustamalla asiakkaitamme ja kansainvälisiä asianajotoimistoja laajoissa ja monimutkaisissa tietoturvaloukkauksissa, olemme tunnistaneet, mitkä ovat tänä päivänä tietoturvaloukkausten kipukohdat ja toisaalta ne tekijät, joiden avulla voidaan tehokkaasti varautua tietoturvaloukkauksiin. Kaikkien aikojen vilkkaimmasta tietoturvaloukkausvuodesta 2022 saatujen kokemusten perusteella ennustamme riskien ja kyberhyökkäysten kasvun vain jatkuvan. Tiimimme on koonnut tärkeimmät huomiomme viiteen eri osa-alueeseen kyberturvallisuudesta tänä päivänä.

TEKNISET YDINELEMENTIT

Kyberrikolliset tarttuvat usein niin sanottuihin helppoihin kohteisiin. Henkilöstön, asiakkaiden, palveluiden, liikekumppaneiden sekä koko liiketoiminnan ja sen jatkuvuuden turvaamiseksi on välttämätöntä rakentaa vahva tekninen kybersuoja IT-järjestelmiin ja -ympäristöihin. Siksi organisaatioiden on tunnettava mahdolliset uhat, käytettävissä olevat parhaat käytännöt ja lain vaatimukset aina kun IT-järjestelmiä, tuotteita ja palveluita hankitaan ja päivitetään. Meidän on katsottava tulevaan – kyberturvallisuuden on nimittäin jatkuttava järjestelmän, tuotteen ja palvelun koko elinkaaren ajan ja sen jälkeenkin. Tämä edellyttää turvallisuustasojen päivittämistä, seurantaa ja arviointia sekä riittävien ja kestävien sopimusehtojen varmistamista teknologiasopimuksissa.

YHTEISTYÖ

Paraskaan saatavilla oleva kybertiimi ei voi turvata koko organisaatiota ilman tiimityötä. Suuret tietomurrot alkavat usein sähköpostihyökkäyksillä, kuten tietojen kalastelulla, joita on usein vaikea havaita sähköpostitulvien joukosta. Kyberrikolliset hyökkäävät usein joko organisaation haavoittuvimpina pidettyihin henkilöihin, kuten uusiin työntekijöihin, jotka eivät ole vielä kunnolla sisällä organisaation käytännöissä, tai vaikutusvaltaisimpiin henkilöihin, kuten johtoryhmän jäseniin. Yhteistyö ja yhteinen vastuu ovat yksi keskeisistä tekijöistä organisaation suojelemisessa. Tämä tarkoittaa, että kaikkien organisaation jäsenten ja ulkopuolisten kumppaneiden on tehtävä vastuullista yhteistyötä yhteisen päämäärän eteen. Tietosuoja- ja IT-funktiot yhdessä organisaation juristien kanssa ovat keskeisessä asemassa tässä jatkuvassa ennaltaehkäisevässä työssä, joka sisältää laajan kentän erilaisia tehtäviä hankintamenettelyistä ja sisäisistä käytännöistä aina kolmansien osapuolien sopimuksiin ja tietosuojan vaikutustenarviointeihin.

KOULUTUS

Riittävä koulutustaso on tarjottava kaikille organisaation jäsenille. Jokaisen tulee tuntea omaan vastuualueeseensa liittyvät riskit. Kyberuhkien lisäksi organisaatioiden tulee tuntea tietosuoja- ja kyberturvalainsäädäntö, mukaan lukien mahdollinen toimialakohtainen erityissääntely. Seuraukset ja riskit luonnollisesti lisääntyvät, jos tietoturvaloukkauksesta ilmenee, että pakollisia lakisääteisiä vaatimuksia ei ole noudatettu. Useimmissa tapauksissa organisaation johto on vastuussa sovellettavien lakisääteisten vaatimusten noudattamisesta.

SUUNNITTELU

Kyberturvallisuus edellyttää jatkuvaa ennakointia. Suomalaisten johtavien kyberturvallisuusasiantuntijoiden mukaan tietomurtoja tapahtuu ennemmin tai myöhemmin kaikissa organisaatioissa. Siten on ehdottoman tärkeää laatia kattava riskienhallintasuunnitelma sekä tietoturvaloukkauskäytäntö tietoturvaloukkausten seurausten minimoiseksi, mukaan lukien kartoittaa jo hyvissä ajoin tarvittavat ulkoiset neuvonantajat teknisen konsultoinnin ja oikeudellisen neuvonannon osalta. Organisaatiot joutuvat tyypillisesti odottamattomaan tilanteeseen, jossa tietoturvaloukkausilmoitus on tehtävä toimivaltaiselle tietosuojaviranomaiselle tai -viranomaisille 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta. Vaikka ilmoitus voidaan tehdä alustavana ja täydentää myöhemmin, on alustavaa ilmoitusta varten täydennettävien tietojen luettelo melko laaja. Joskus ilmoitus on tehtävä useissa maissa noudattaen toisistaan erilaisia paikallisia ilmoitusprosesseja. Olemassa oleva kansainvälisistä asianajotoimistoista ja muista asiantuntijoista koostuva verkostomme kattaa kaikki lainkäyttöalueet maailmanlaajuisesti ja mahdollistaa näiden velvoitteiden täyttämisen asetetuissa aikavaatimuksissa.

HUOLENPITO JA VÄLITTÄMINEN

Kyberriskit ja niiden realisoituminen aiheuttavat huolta organisaatioille, niiden henkilökunnalle ja asiakkaille. Tietoturvaloukkaus, johon liittyy yksilöiden henkilötietoja, voi olla shokki loukkauksen kohteena oleville rekisteröidyille. Kun resursseja allokoidaan organisaatiossa tietoturvaloukkauksen selvittämiseksi, ulkoiset neuvonantajat voivat olla suureksi avuksi, kun osa sisäisistä resursseista on kohdistettu organisaation ja yksilöiden tukemiseen. Kyberriskien hallinta ei ole vain liiketoiminnan suojelemista, vaan myös yksilöistä, heidän turvallisuudestaan ja hyvinvoinnistaan huolehtimista.

Tämä artikkeli on julkaistu 30. maaliskuuta 2023 Dittmar & Indreniuksen Quaterly-julkaisussa.
Linkki alkuperäiseen artikkeliin: www.dittmar.fi/insight/elements-of-cybersecurity/

D&I:N KYBERTURVALLISUUDEN TARKISTUSLISTA ORGANISAATIOILLE

1 Toteuta kattavat tekniset kyberturvallisuustoimenpiteet hankkimalla hyvät IT-järjestelmät ja pitämällä ne ajan tasalla. Harkitse huippuluokan salausta ja salausavainten hallintaa, etenkin kun käsitellään salasanoja tai arkaluonteisia tietoja. Kiinnitä huomiota tietojen saatavuuden ja eheyden varmistamiseen, mukaan lukien varmuuskopioihin ja lokitietoihin.

2 Laadi kattava riskienhallintasuunnitelma ja tietoturvaloukkauskäytäntö, jotta voit reagoida tehokkaasti mahdollisiin tietoturvaloukkauksiin. Varmista ylimmän johdon tietoisuus ja osallistuminen.

3 Osallista organisaatiosi jäsenet kyberturvallisuuteen heidän roolinsa ja tehtäviensä mukaisesti.

4 Kartoita ja ota yhteyttä ulkoisiin neuvonantajiisi etukäteen, jotta voit toimia nopeasti tietoturvaloukkauksen sattuessa.

5 Kouluta organisaatiotasi suojaamaan yksilöitä, liiketoimintaa ja päivittäistä toimintaa, mukaan lukien tunnistamaan ja estämään kyberhyökkäyksiä ja esimerkiksi tietojen kalasteluyrityksiä. Osoita, että välität molemmista – yksilöiden turvallisuudesta ja liiketoiminnan jatkumisesta. ■

JUKKA LÅNG, JOHANNA TUOHINO JA JULIA VIKSTRÖM

- Jukka Lång
  Partner
- Johanna Tuohino
  Senior Associate
- Julia Vikström
  Associate

DITTMAR & INDRENIUS

KYBERKANSALAISTAIDOT – MIKÄ ON NIIDEN MERKITYS JA MITEN NIITÄ TULISI KEHITTÄÄ EU:SSA?

// Marianne Lindroth

Kyberturvallisuustaidoista on keskusteltu paljon viime vuosina, ja erityisesti kyberturvallisuuden ammattilaisten osaamisprofiilit on määritelty myös EU:n tasolla. Kyberkansalaistaitojen kehittäminen on kuitenkin ensiarvoisen tärkeää sekä EU:n kollektiivisen resilienssin että yksilöiden resilienssin kannalta. EU:n laajuisella Cyber Citizen -hankkeella pyritään luomaan yhteinen malli kansalaisten kouluttamiseksi kyberturvallisuustaidoissa, ottaen huomioon eri kohderyhmien erilaiset tarpeet ja kyberalan kehittyvät uhat. Mallin avulla kehitetään kaikille EU:n kansalaisille kyberturvallisuuden oppimisportaali, johon sisältyy kyberturvallisuuden taitopeli.

HANKE KAIKILLE EUROOPPALAISILLE

Kyberkansalaistaitojen kehittämishanke Cyber Citizen vastaa käytännön tarpeeseen luoda turvallisuuskulttuuria ihmiskeskeisessä digitaalisessa ympäristössä. Hankkeen tavoitteena on kehittää kaikille eurooppalaisille yhteinen malli kyberkansalaistaitojen oppimiseksi kaikkialla Euroopan unionissa. Hanketta rahoittaa EU:n elpymisväline, sen tilaajana on liikenne- ja viestintäministeriö ja toteuttajana Aalto-yliopisto.

Kaiken kaikkiaan Cyber Citizen -hankkeella luodaan kyberturvallisuuden oppimisen eurooppalainen malli, joka puolestaan vahvistaa Euroopan kyberturvallisuutta ja tuottaa yhteisiä käytäntöjä. Mallin pohjalta rakennetaan digitaalinen oppimisportaali. Tässä portaalissa hyödynnetään monenlaisia verkko-oppimismenetelmiä. Olennainen osa portaalia on kyberturvallisuuspeli, joka tarjoaa tietoa ja ymmärrystä viihdyttävällä tavalla.

Hankkeen ensimmäisessä vaiheessa tutkittiin kyberkansalaistaitojen koulutuksen nykyisiä opetusmenetelmiä, näkemyksiä ja materiaaleja kaikissa Euroopan unionin jäsenmaissa. Tähän sisältyi jäsenvaltioiden kansallisia ominaispiirteitä ja vaatimuksia. Myös EU:n virallisia politiikkoja tarkasteltiin. Lisäksi pelianalyysi, kyberturvallisuusindeksien arviointi ja kirjallisuuskatsaus olivat osa tutkimusta. Käytetyt tiedot kerättiin useista eri lähteistä.

KOHTI YHTENÄISTÄ, IHMISKESKEISTÄ LÄHESTYMISTAPAA

Raportti osoittaa, että kybertaitojen kehittämisessä on suuria eroja eri puolilla EU:ta ja että kaikkien jäsenvaltioiden kansalaiset hyötyisivät yhtenäisemmästä ja ihmiskeskeisemmästä lähestymistavasta kyberturvallisuuteen.

Kyberturvallisuusuhat lisääntyvät kaikissa Euroopan unionin maissa. Tämän kasvavan uhan torjumiseksi kansalliset hallitukset eri puolilla EU:ta ovat investoineet ohjelmiin, joilla parannetaan kansalaisten kybertaitoja. Kyberturvallisuustietoisuudessa ja -koulutuksessa on kuitenkin merkittäviä eroja. Vaikka kyberturvallisuus on kansainvälinen uhka, tällä hetkellä ei ole olemassa yhteistä mallia kyberturvallisuuden oppimiselle tai käytännölle.

"Kyberkansalaistaidot" ovat perinteisesti keskittyneet pitkälti teknologiaan, ja tutkimuksen perusteella ymmärrystämme kybertaidoista tulisi päivittää ihmiskeskeisemmäksi. Aalto-yliopiston kyberturvallisuuden professori ja Cyber Citizen -hankkeen johtaja Jarno Limnéll vertaa ihmiskeskeistä lähestymistapaa liikennesääntöjen ymmärtämiseen autoa ajaessa:

"Kansalaisten kyberturvallisuus koostuu heidän tiedoistaan, taidoistaan ja asenteistaan. Pelkkä teknologian hallitseminen ei riitä kyberturvallisuuteen. Samoin autolla ajaminen ei riitä turvallisuuteen; Sinun on myös tunnettava säännöt ja erilaiset tilanteet sekä oltava tietoinen muista tienkäyttäjistä. Sen lisäksi, että kyberkansalaistaidot ovat välttämättömiä sujuvan ja turvallisen jokapäiväisen elämän kannalta, ne ovat välttämättömiä myös koko EU:n turvallisuuden ja taloudellisen menestyksen kannalta."

EU:n jäsenvaltioiden kyberturvallisuuskulttuuria rakennetaan parhaillaan. Kulttuurin luominen ja vahvistaminen vie aikaa, ja siksi on tärkeää työskennellä määrätietoisesti. Tästä syystä tarvitsemme kiireellisesti Cyber Citizen -hankkeen kaltaisia toimia.

Ajan myötä voimme nostaa yhteisen ymmärryksen ja laajan osaamisen yhteiseksi kulttuuriksi, jolla on suuri merkitys koko yhteiskunnan ja sen kansalaisten tulevaisuudelle.

TUTKIMUKSEN PÄÄKOHDAT

Tutkimus osoitti, että EU:n jäsenmaissa on selkeä halukkuus kehittää kyberturvallisuuden kansalaistaitoja ja tukea elinikäistä oppimista. Yhteinen malli auttaisi tämän saavuttamisessa.

EU-maiden kyberturvallisuutta koskevat koulutuspoliittiset suuntaviivat ovat suhteellisen uusia, minkä vuoksi niiden vaikutuksia on tässä vaiheessa vaikea arvioida. Selvää edistystä on kuitenkin tapahtunut, ja asian tärkeys tunnustetaan. Kyberturvallisuutta ei enää pidetä yksinomaan ammattilaisten vastuulla. Sen sijaan se on olennainen osa kaikkea sosiaalista toimintaa.

Kybertoimintaympäristöstä on tullut monimuotoisempi ja monikäyttöisempi, mikä ymmärretään nyt paremmin Euroopan unionissa. Nykytilanne korostaa entistä enemmän jatkuvan oppimisen merkitystä sekä tarvittavien tietojen ja taitojen laajuutta. Kyberkansalaistaidot on ymmärrettävä dynaamisina taitoina, jotka muuttuvat kontekstin ja ympäristön mukana, eikä valppauden lisäksi voida korostaa liikaa elinikäisen oppimisen tarvetta.

Jokaisella tulisi olla kyberturvallisuuden perustaidot. Inhimilliseen osaamiseen ja sivistykseen perustuvan turvallisuuskulttuurin kehittymistä tulee määrätietoisesti vahvistaa. Kaikilla ikäryhmillä on erilainen osaamistaso diginoviiseista digiguruihin. Kysymys kuuluu, miten eri kohderyhmät otetaan huomioon. Perusosaaminen ja kyberturvallisuuden yleinen taso vaihtelevat suuresti Euroopan unionin jäsenmaissa. Tästä kertoo suuri vaihtelu kyberturvallisuuden tasoa mittaavissa indekseissä ja näkemyksissä siitä, miten kyberturvallisuuden osaamista ja kulttuuria voidaan parantaa.

Ihmiset ovat erilaisia, oppivat eri tavalla ja heillä voi olla erilaisia rajoitteita, ja siksi kyberturvallisuuskoulutuksessa ei ole löydettävissä yhtä yleispätevää ratkaisua. Tällä hetkellä eri kohderyhmien välisiä eroja ei ole vielä riittävästi huomioitu eri EU-maissa.

Kyberturvallisuuden koulutusmateriaalien tarjonta vaihtelee sekä laadultaan että sisällöltään, ja koulutusten järjestämisvastuuta on jaettu eri tavoin. Tämä vaikuttaa suoraan siihen, kuinka laajasti ja millä tavoin koulutusta on tarjolla ja kuinka todennäköisesti kansalaiset osallistuvat siihen. Korkeatasoista kyberturvallisuuskoulutusta ja siihen liittyvää yhteistyötä tulee lisätä ja päällekkäistä työtä vähentää. Yksi Cyber Citizen -aloitteen tavoitteista on edistää koulutuksen harmonisointia ja järkeistämistä.

Monissa EU-maissa digitaalisia taitoja, myös kyberturvallisuustaitoja, koskeva koulutus perustuu kansalaisten digitaalisten taitojen eurooppalaiseen viitekehykseen (DigComp). On hyvä, että taustalla on yhteinen kehys, sillä se helpottaa yhteisen koulutusmallin kehittämistä. Kyberturvallisuustaidot ovat tietenkin vain yksi osa DigCompia ja siksi niitä on syvennettävä ja hiottava.

Kyberturvallisuuden työvoimapula vaikuttaa myös kansalaisten koulutukseen, sillä ammattilaisia tarvitaan kansalaisten kouluttamiseen ja koulutuksen sisällön suunnitteluun. Tämä ongelma on tunnustettu laajemmin ja sen ratkaisemiseksi toteutetaan erilaisia toimenpiteitä. On kuitenkin tärkeää korostaa asian kiireellisyyttä.

Pelit ovat vakiinnuttaneet asemansa sosiaalisen käyttäytymisen muotona, ja niistä on tulossa yhä tärkeämpi oppimisväline. Tämä havainto tukee Cyber Citizen -aloitteen ajatusta pelinkehityksestä ja pelillistämisen hyödyntämisestä oppimisessa myös oppimisportaalissa.

KYBERKANSALAISTEN TAIDOT

Osana tutkimusta määriteltiin kyberkansalaisten (Cyber Citizen) taidot. Kyberkansalainen on EU:n jäsenvaltiossa pysyvästi tai tilapäisesti asuva henkilö, joka käyttää digitaalisia palveluita tai hyötyy niiden tuottamisesta. Kyberkansalaisten taidot koostuvat kyberympäristössä tarvittavista tiedoista, taidoista ja kyvyistä. Se koostuu komponenteista, jotka auttavat ihmisiä kehittämään ja ylläpitämään tietojaan ja taitojaan tavalla, joka antaa heille tarvittavan kyvyn ja motivaation toimia järkevästi eri elämäntilanteissa. Kyberkansalaisten taidot tarkoittavat henkilökohtaisen ja sosiaalisen vastuun ottamista ja tämän vastuun merkityksen ymmärtämistä kyberympäristössä.

Euroopan unionissa tarvitaan yhteinen määritelmä kyberkansalaisten taidoille ja tapoja mitata taitotasoa. Kyberkansalaisten taidot ymmärretään eri tavoin eri puolilla EU:ta, ja vain osa jäsenmaista on määritellyt niitä ollenkaan. Määritelmät voivat olla lähes identtisiä, mutta kansallisten ja kulttuuristen erojen vuoksi niitä tulkitaan eri tavoin.

Eurooppalaisella kansalaisten digitaalisten taitojen puitekehyksellä (DigComp) on merkittävä vaikutus useimmissa jäsenmaissa. Tästä syystä Cyber Citizen -tutkimusryhmä tunnisti konkreettisia kyberkansalaisten taitoja, jotka tukevat DigComp-viitekehyksen käyttöönottoa EU:ssa. Kyberturvallisuusosaamista löytyy kaikilta DigCompin osaamisalueilta, joita ovat informaatio- ja datalukutaito, viestintä ja yhteistyö, digitaalisen sisällön luominen, turvallisuus ja ongelmanratkaisu.

KOHTI TURVALLISEMPAA JA SUOJATUMPAA EUROOPPAA

Kun kansalaisilla on hyvä asenne ja osaamiseen perustuva turvallisuuden tunne, ovat he halukkaampia käyttämään digitaalisia palveluita. Tällä tavoin Euroopan unionista tulee kestävämpi, kilpailukykyisempi ja riippumattomampi. Kansalaisoppimisen mahdollisuudet luovat ymmärrystä ympäristöstä, toimijoista ja prosesseista, jotka vaikuttavat jokaisen digitaaliseen elämään. Parantamalla henkilökohtaisia taitojamme henkilökohtaiset ja kollektiiviset kykymme parantavat itseluottamustamme. Hankkeen toisessa vaiheessa luodaan tutkimusraportin ja erityisesti kyberkansalaisten osaamiskehyksen pohjalta kyberkansalaisten osaamisen oppimiskonsepti. Kolmannessa vaiheessa suunnitellaan oppimiskonseptin mukainen oppimisportaali.

Oppimisportaalissa on sisältöä kaikille kansalaisille, ja tämä sisältö, kuten kyberkansalaistaitojen oppimispeli, huomioi eri kohderyhmät. Kansalaisten valmiuksia toimia turvallisesti digitaalisessa maailmassa parannetaan oppimisportaalin opetuksellisilla ja viestinnällisillä elementeillä. Kansalaisia pyydetään osallistumaan koulutussisältöjen suunnitteluun. Koulutuksen saatavuus ja saavutettavuus on tärkeää, kun Euroopan unioniin luodaan osaamisen parantamiseen perustuva yhteinen kyberturvallisuuskulttuuri.

KYBERKANSALAISTEN OSAAMISEN YHTEISTYÖVERKOSTO

EU:n eri jäsenmaiden hankkeiden ja käytäntöjen moninaisuus tarkoittaa, että joka puolelta Eurooppaa on opittavaa. Cyber Citizen -hankkeella luodaan parhaillaan Euroopan laajuista yhteistyöverkostoa, johon ovat tervetulleita kaikki kyberkansalaisuuden taitojen kehittämisestä kiinnostuneet.

Näkemyksiä kyberkansalaisten taidoista ja niiden kehittämisestä oppimismallin ja -portaalin avulla keskustellaan kaikkien EU-maiden kanssa, ja asiantuntijoita kutsutaan esimerkiksi työpajoihin keskustelemaan parhaista ratkaisuista ja tarjoamaan asiantuntemustaan. Tulevaisuudessa myös kansalaiset otetaan mukaan sisällön suunnitteluun. Tavoitteena on luoda jotain uutta ja kiinnostavaa kaikille EU-kansalaisille sekä herättää kiinnostusta kyberturvallisuuteen.

Yhteenvetona voidaan todeta, että hankkeen tavoitteena on luoda oppimismalli, julkaista oppimisportaali, joka sisältää pelin, rakentaa Euroopan laajuinen kyberkansalaisten osaamisen sidosryhmien verkosto ja lisätä tietoisuutta kyberkansalaisten taidoista ja niiden merkityksestä sekä kansalaisten että poliittisten päättäjien keskuudessa. Siksi tutkijat pyytävät kaikkia kyberturvallisuuden, siihen liittyvän tutkimuksen tai koulutuksen parissa toimivia tai keitä tahansa, jotka uskovat että heillä on annettavaa, liittymään Cyber Citizen -hankeverkostoon. ■

MARIANNE LINDROTH

- Hankkeen johtaja, Kyberturvallisuus-tietoisuus, koulutus ja harjoittelu
- Kyberkansalaisaloite
- Aalto Yliopisto, Kyberturvallisuus

CYBER CITIZEN

Aalto University

KYBERTURVALLISUUDEN AMMATTILAISTEN KOULUTUS

// Martti Lehto

Kyberturvallisuusalalla osaajapula on valtava. Tutkimustulokset osoittavat selvästi, että nykyinen kyberammattilaisten määrä ei riitä kattamaan kaikkia kyberturvallisuuden rekrytointitarpeita. Kyberturvallisuuskoulutukseen tarvitaan korkeakoulujen välistä yhteistyötä, kolmannen sektorin tukea ja julkisen tahon panostuksia.

JOHDANTO

Suomi on maailman johtava digitalisaation hyödyntäjä korkeakoulutuksessa ja siihen perustuvassa jatkuvassa oppimisessa. Tavoitteena on, että opetussisällöt avataan mahdollisimman laajasti käyttöön. Osaamisen uudistamisen kasvavien tarpeiden vuoksi tulisi jatkuvan oppimisen painottua yhä enemmän korkeakoulujen koulutustehtävässä.

Maailmanlaajuisesti on tunnistettu pula osaavista kyberturvallisuusasiantuntijoista. Osaajapulan kannalta on otettava huomioon erilaiset osaamistarpeet eri tehtävissä. Kyberturvallisuuden tietojen, taitojen ja kykyjen osalta osaamiskenttä on melko laaja ja osaajan pitää erikoistua johonkin tiettyyn kokonaisuuteen. Tämä on otettava huomioon koulutuksessa, eli mihin tehtävään valmistuvan osaajan oletetaan työllistyvän. Toki on selvää, että koulutuksen kautta saavutetaan tietty perusosaaminen ja myöhemmin työtehtävien, erikoistumisen ja mahdollisten erikoiskoulutusten kautta saavutetaan syvempi erikoisasiantuntijuus kyseiseen aihealueeseen.

KYBERTURVALLISUUSKOULUTUS AMMATTIKORKEAKOULUISSA

Ammattikorkeakouluissa annettava kyberturvallisuusopetus (AMK- ja YAMK-korkeakoulututkinto, sekä erikoistumis- täydennys- ja muuntokoulutus) on sisällöllisesti kattavaa ja kykenee modulaarisen rakenteen perusteella muuntautumaan teollisuuden tarpeisiin. Tieto- ja viestintätekniikan sekä tietojenkäsittelyn tutkinto-ohjelmien sisällä tarjotaan kyberturvallisuuden koulutusta.

Opetussuunnitelmarakenteet ovat eri luokkia sen suhteen, onko kyberturvallisuus sijoitettu pakollisiin, erikoistumis- (tai ammatillisiin opintoihin) vai vapaasti valittaviin opintoihin. Tärkeimpiä ovat kyberturvallisuuteen tähtäävät koulutusohjelmat ja koulutusohjelmat, joiden sisällä tarjotaan kyberturvallisuuden erikoistumisopintoja. Tämän luokituksen perusteella YAMK-tason neljä koulutusohjelmaa löytyy kolmessa ammattikorkeakoulussa:

- JAMK, Master's Degree in Information Technology, Cyber Security, Insinööri
- TurkuAMK, Ohjelmistotekniikka ja ICT
- Insinööri
- Tradenomi
- XAMK, Kyberturvallisuus, Insinööri

AMK-ohjelmat koostuivat monimutkaisista opetussuunnitelmarakenteista. Joissakin ammattikorkeakouluissa opetussuunnitelmat on laadittu siten, että opiskelijoille on tarjolla paljon kursseja valittavaksi. Vaihtoehtoisesti erikoistuminen on rakennettu yhdeksi opetussuunnitelmaksi, josta opiskelijat voivat tehdä modulaarisia valintoja. Neljä ammattikorkeakoulua tarjoaa AMK-tason kyberturvallisuuden koulutusohjelman:

- JAMK, tieto- ja viestintätekniikka, insinööri
- Laurea, tietojenkäsittely, kyberturvallisuus, tradenomi
- TurkuAMK
- Tieto- ja viestintätekniikka, insinööri
- Tietojenkäsittely, tradenomi
- XAMK, kyberturvallisuus, insinööri

Tällä hetkellä ammattikorkeakoulujen kyberturvallisuuteen painottuvassa koulutuksessa sisäänotto on noin 555 (165 tutkinto-opiskelijaa ja 390 sivuaineopiskelijaa). Lisää kyberturvallisuuden asiantuntijoita tarvitaan vastaamaan jatkuvasti laajenevan digitalisaation vaatimuksiin. Tämän seurauksena kyberturvallisuusosaamista tarvitaan yhä enemmän eri digitalisoituvilla toimialoilla.
Koulutuksen resursseja pohdittaessa tulee myös muistaa, että ammattikorkeakoulut tarjoavat pääsääntöisesti teknistä kyberturvallisuuskoulutusta, joka tähtää tekniseen osaamiseen. Tällainen insinööriopetus vaatii laajoja ja monimutkaisia oppimisympäristöjä, joiden hankkiminen ja ylläpito on kallista. Riittävän teknisen osaamisen takaamiseksi resurssien allokoinnissa tulee huomioida tarvittavien oppimis- ja koulutusympäristöjen hankinta-, kehitys- ja ylläpitokustannukset.

KYBERTURVALLISUUSKOULUTUS YLIOPISTOISSA

Kyberturvallisuuteen keskittyneiden koulutusohjelmien määrä on pieni ja opetus on keskittynyt maisteritasolle. Yliopistot tuottavat suhteellisen vähän kyberturvallisuuden asiantuntijoita suhteessa havaittuun osaamispulaan. Suuri osa koulutusohjelmista on integroinut kyberturvallisuuden tutkintorakenteeseen valinnaisina tai pakollisina opintoina 1-15 opintopisteen suuruisina Yliopistot tarjoavat vähän täydennyskoulutusta kyberalalla. Seuraavassa taulukossa on esitetty kyberturvallisuuskoulutuksen (pää- ja sivuaine) sisältävät koulutusohjelmat:

Yliopisto	Koulutusohjelmat/Kurssimoduulit	Sisäänotto 2022
Aalto yliopisto	Security and Cloud Computing (Security)	11
Aalto yliopisto	Security and Cloud Computing (SECCLO)	76
Helsingin yliopisto	Tietojenkäsittelytieteen maisteriohjelma	45
Tampereen yliopisto	Suuntaus: Advanced Studies in Information Security	1-30
Tampereen yliopisto	Master's Programme in Security and Safety Management: Safety Management and Engineering	8
Tampereen yliopisto	Master's Programme in Security and Safety Management: Security Governance	8
Jyväskylän yliopisto	Kyberturvallisuuden maisteriohjelma	45
Jyväskylän yliopisto	Turvallisuuden ja Strategisen analyysin maisteriohjelma	25
Turun yliopisto	Cyber Security -pääaine + EIT Digital Master School kaksoistutkinto-ohjelma	35
Turun yliopisto	Cryptography -pääaine	5
Turun yliopisto	Tietoliikenne- ja kybertuvallisuusteknologia -pääaine	6-8
Oulun yliopisto	Tietotekniikka TkK + DI	100
Åbo Akademi	Temaattinen moduuli: Safety-Critical and Autonomous Systems	n/a
Itä-Suomen yliopisto	Tietojenkäsittelytiede LuK + FM	68
Vaasan yliopisto	Automaatio ja tietotekniikka TkK + DI	52
LUT yliopisto	Tietotekniikka TkK + DI	82

Listauksesta nähdään, että kyberturvallisuuteen keskittyviä tutkinto-ohjelmia on suhteellisen vähän. Yliopistojen tarjoamat kyberturvallisuuden tutkinto-ohjelmat tai läheisesti alaan liittyvät tutkinto-ohjelmat eroavat sisällöllisesti toisistaan. Yliopistoilla on toisin sanoen omat erikoistumisalansa kyberturvallisuudesta. Lisäksi huomionarvoista on se, että opetus on keskittynyt ylempiin korkeakoulututkintoihin. Yksittäisiä kyberturvallisuuden opintoja on yleisesti tarjolla lukuisissa tutkinto-ohjelmissa pakollisina- tai valinnaisina opintoina.

Kyberturvallisuuden ja turvallisuuden koulutusohjelmien arvioitu kokonaissisäänotto on noin 250 (110 pääaineena, 140 sivuaineena) vuonna 2023. Yllä mainittu luku sisältää vain kyberturvallisuuden ja turvallisuuden koulutusohjelmien aloitushaun, eikä siten sisällä niihin liittyvien alojen tutkintoja, esim. tietojärjestelmätiede. Yliopistojen tuottamien asiantuntijoiden määrä on kaiken kaikkiaan suhteellisen pieni, kun otetaan huomioon havaittu osaamispula.

MUIDEN KOULUTUSTARJOAJIEN KYBERTURVALLISUUSKOULUTUS

Ei-tutkintoon tähtäävää kyberturvallisuuskoulutusta on Suomessa saatavilla, mutta tällä hetkellä vallitsee eräänlainen kohtaanto-ongelma. Ne, jotka koulutusta eniten tarvitsisivat, eivät löydä sitä, eivätkä hakeudu siihen. Esimerkiksi senioreille suunnattua koulutusta on vähän tarjolla.

Kolmannella sektorilla laajinta kyberturvallisuuteen liittyvää koulutusta järjestää Maanpuolustuskoulutusyhdistys (MPK). Lisäksi jotkin aikuiskoulutuskeskukset tarjoavat kyberturvallisuuteen liittyvää koulutusta.

Lapset ja nuoret saavat tällä hetkellä kyberturvallisuuskoulutusta osana koulutuspolkuaan sekä perus- ja toisen asteen koulutuksessa että myöhemmissä opinnoissa. Kuitenkin ne, jotka ovat suorittaneet opintonsa aikana, jolloin kyberturvallisuus ei kuulunut peruskoulutukseen tai jatko-opintoja, voivat tällä hetkellä jäädä kokonaan kyberturvallisuuskoulutuksen ulkopuolelle, jos he eivät saa sitä työpaikallaan.

Yrityksille ja muille organisaatioille kouluttajia on Suomessa melko paljon. Suuryritysten ja julkisten organisaatioiden työntekijät saavat yleensä työnsä yhteydessä koulutusta, mutta pk-yritysten työntekijät, itsensä työllistäjät ja yrittäjät voivat jäädä sitä ilman. Toinen ongelma voi olla se, että pk-yritysten johto tai yrittäjät eivät tunnista koulutuksen tarvetta.

KYBERTURVALLISUUDEN ASIANTUNTIJOIDEN MÄÄRÄLLINEN TARVE

Elinkeinoelämä, viranomaiset ja kolmas sektori tarvitsevat uusia kyberammattilaisia. Liikenne- ja viestintäministeriön kyberosaamistarpeita kartoittavassa kyselyssä 73 % vastaajista näkee organisaatioissaan merkittävää osaajapulaa. Lähes kaikki vastaajat ottaisivat uusia ammattilaisia, jos heitä vain saisi. Kyselyn perusteella tarpeet vaihtelevat voimakkaasti. Osaamistarve-esiselvityksessä pienelle ryhmälle (16 %) vastaajista osaamisvaje vaaransi toiminnan turvallisuuden tai kannattavuuden. Kyse ei ole enää kasvun heikkenemisestä vaan peräti elinkelpoisuudesta.

Kysyntä on kova myös kyberturvallisuusalan sisällä. Kyberalan (FISC) kyselyn mukaan alan yrityksistä 87 % aikoi palkata kyberturvallisuusalan henkilökuntaa. Kyberalan jäsenkyselyn perusteella noin 35 % vastaajista ilmoitti osaavan työvoiman puutteen olevan merkittävin alan kasvua rajoittava tekijä.

Ammattitaitopula on todellisuutta, vaikka sen tasoa on vaikea ennustaa tarkasti. Nykyisten tietojen perusteella arvioidaan, että Suomi tarvitsee lähivuosina 5 000–8 000 kyberturvallisuuden ammattilaista. Lisäksi 1 000–5 000 uutta ammattilaista tarvitaan työskentelemään kyberturvallisuuden parissa muun työnsä ohella. Kaikki nämä ihmiset tarvitsevat koulutusta.

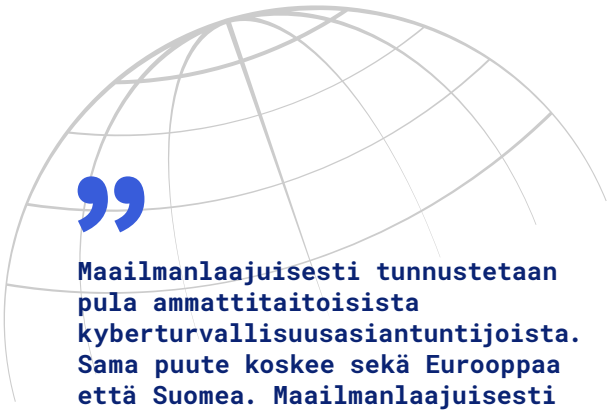
Yrityksillä on monenlaisia osaamistarpeita. Osaamisprofiili voidaan määritellä yleisesti käytetyn NCWF-luokituksen perusteella. Tätä yhdysvaltalaista viitekehystä on käytetty laajasti kuvaamaan kyberturvallisuuteen liittyviä osaamisen pääluokkia ja osaamiskategorioita sekä näiden alla olevia erityisosaamisaloja. Tutkimuksen mukaan yritysten määrälliset tarpeet vaihtelevat eri osaamisalueilla. Turvalliseen tuotantoon tarvitaan eniten uusia osaajia. Tämä 6 000–13 000 uuden kyberammattilaisen tarve jakautuu pääkoulutusalan mukaan seuraavasti:

1. Turvallinen tuotanto 900–1 500 uutta henkilöä,
2. Operointi ja ylläpito 700–1 100 henkilöä,
3. Kokonaisuuden valvonta ja johtaminen 800–1 300 henkilöä,
4. Suojaaminen ja puolustus 900–1 400 henkilöä,
5. Analysointi 600–1 000 henkilöä,
6. Tiedonkeruu ja operointi 500–800 henkilöä,
7. Tutkinta 500–800 henkilöä.

Tutkimus osoittaa, että erityisiä tarpeita oli (a) valvonnassa ja hallinnassa (erityisaloilla, kuten järjestelmäarkkitehtuuri, kyberturvallisuuden hallinta, strategiat ja strategioiden parissa työskentelevät kyber- tai tietoturvapäälliköt) sekä (b) operatiivisessa osaamisessa, jossa painottuu järjestelmien suojaus sekä sitä tukeva analyysi. Julkinen sektori hakee suhteellisesti enemmän laaja-alaisen osaamisen johtajia ja riskinhallintaosaajia, kun taas elinkeinoelämä hakee enemmän hallinto- ja arkkitehtuuriosaajia.

Osaamistarve on jakautunut melko tasaisesti kaikille kyberturvallisuuden osaamisalueille. Tämä tarkoittaa kokonaisvaltaisen koulutuksen tarvetta. Korkeakoulujen tutkinto-opintojen sekä muunto- ja täydennyskoulutuksen tulee kattaa kaikki nämä osa-alueet vastatakseen osaamistarpeisiin.

Elinkeinoelämä, viranomaiset ja kolmas sektori tarvitsevat uusia kyberammattilaisia. Liikenne- ja viestintäministeriön kyberosaamistarpeita kartoittavassa kyselyssä 73 % vastaajista näkee organisaatioissaan merkittävää osaajapulaa. Lähes kaikki vastaajat ottaisivat uusia ammattilaisia, jos heitä vain saisi.



Maailmanlaajuisesti tunnustetaan pula ammattitaitoisista kyberturvallisuusasiantuntijoista. Sama puute koskee sekä Eurooppaa että Suomea. Maailmanlaajuisesti ammattitaitoisen työvoiman tarve on miljoonia; Suomen osalta voidaan sanoa, että se on useita tuhansia.

JOHTOPÄÄTÖKSIÄ

Kyberturvallisuudessa yksi tärkeimmistä ja arvokkaimmista asioista on ammattitaitoinen henkilöstö. Riippumatta teknisistä ratkaisuista ja prosesseista organisaatiossa, sillä ei ole kybersietokykyä ilman ammattitaitoista henkilöstöä. Tämä koskee kaikkia työtehtäviä, koska henkilöstön epäpätevyys tai tiedon puute voi altistaa organisaation haavoittuvuuksille kybertoimintaympäristössä.

Maailmanlaajuisesti tunnustetaan pula ammattitaitoisista kyberturvallisuusasiantuntijoista. Sama puute koskee sekä Eurooppaa että Suomea. Maailmanlaajuisesti ammattitaitoisen työvoiman tarve on miljoonia; Suomen osalta voidaan sanoa, että se on useita tuhansia.

Tähän osaamispulaan liittyen on tärkeää ottaa huomioon eri työtehtävissä tarvittavat erilaiset taidot. Kyberhyökkäysten tunnistaminen ja tapausten hallinta edellyttää erilaista kyberturvaosaamista kuten kyberturvallisuuden hallinta tai uusien järjestelmien hankinta. Tämä on otettava huomioon koulutuksessa, eli mihin työtehtäviin valmistuvien opiskelijoiden odotetaan työllistyvän. Tietenkin tulee muistaa, että koulutus antaa tiettyjä perusosaamisen, jota voidaan myöhemmin kehittää syvemmäksi osaamiseksi työtehtävien, erikoistumisen ja mahdollisen alan erikoiskoulutuksen kautta.

Kyberturvallisuuskoulutus tulee myös kohdistaa työelämän eri osa-alueille. Näin tarvittavat taidot olisivat yleisesti yhteiskunnan saatavilla. Myös tutkintoja päivittävä täydennyskoulutus vaatii opetusresursseja. Koulutuksen tulee tuottaa tarpeeksi asiantuntijoita, jotta yhteiskunta on valmis vastaamaan nykymaailman haasteisiin.

Kyberturvallisuuden asiantuntijoiden määrää yhteiskunnassa voidaan lisätä useisiin tekijöihin vaikuttamalla. Yksi tapa on lisätä alan koulutusohjelmien määrää ja aloittamista. Tämä edellyttää henkilöresurssien lisäämistä. Lisäksi kyberturvallisuuden asiantuntijoiden määrää voidaan lisätä kehittämällä täydennyskoulutusta. Lisäksi korkeakouluorganisaatioiden välisen koulutusyhteistyön parantaminen mahdollistaisi opiskelijoille entistä monipuolisempia erikoistumisaloja kyberturvallisuuden eri osa-alueilla.

Kyberturvallisuuskoulutuksen sisäänottovahvuuksien nostaminen edellyttää resursseja sekä koulutukseen että tutkimukseen. Haasteena on nopealla aikataululla saada rekrytoitua tutkijoita ja opettajia korkeakouluihin.

Muissa EU-maissa on luotu toimivia yhteistyöverkostoja yritysten, kyberturvallisuuskoulutusta koordinoivien valtiollisten tahojen sekä kolmannen sektorin toimijoiden kanssa. Suomi hyötyisi myös kansalaisten kouluttamisesta ja koulutusyhteistyötä koordinoivan toimielimen johdolla toimivasta kansalaisten kyberturvataitojen kehittämisen yhteistyöverkostosta. Yhteistyöverkostoa voisi hyödyntää kyberkoulutukset kokoavan verkkosivuston suunnittelussa ja kansalaisen kyberturvallisuuskonseptin jatkokehityksessä.

Askel oikeaan suuntaan on otettu, kun opetus- ja kulttuuriministeriö on rahoittanut vuonna 2022 alkanutta kyberturvallisuuskoulutuksen kehittämisen ja saatavuuden lisäämisen ohjelmaa. Kyseessä on Jyväskylän yliopiston ja Jyväskylän ammattikorkeakoulun koordinoima laaja yhteistyöhanke. Hanke kokoaa verkoston kehittämään, koordinoimaan ja tarjoamaan kyberturvallisuuden korkeakoulutusta. Siihen osallistuu yhdeksän yliopistoa ja 11 ammattikorkeakoulua sekä verkostoyliopisto FiTECH. ■

MARTTI LEHTO

Työelämäprofessori,
Jyväskylän yliopisto

Artikkeli perustuu Valtion kyberturvallisuusjohtaja Rauli Paanaselle vuonna 2022 tehtyyn raporttiin: Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushanke, JYU tutkimuspaperi 93/2022

secapp

VARAUDU | HÄLYTÄ | VIESTI | DOKUMENTOI

"Jos osaa älypuhelinta käyttää, osaa käyttää myös tätä sovellusta."

- Teemu Pesonen, Komatsu Forest

Jokainen sekunti merkitsee

Auttaa turvaamaan päivittäistä toimintaa, hallitsemaan kriisejä ja pelastamaan ihmishenkiä.

Parantaa kentällä tai yksin työskentelevien työntekijöiden turvallisuutta – hälyttää myös apua ellei henkilö itse pysty.

Hälyttäminen, koordinointi, nopea tilannekuva ja mobiili raportointi käden ulottuvilla.

Haluatko tietää lisää?

myynti@secapp.fi

secapp.fi

KVARTAALIKATSAUS Q1/2023

// Timo Rinne

SISÄLLYS:

ALUSTUS

NIS2- ja CER-direktiivit kiihdyttävät EU-maiden kyberturvatalkoita. Erityisesti NIS2-direktiiviin liittyviä toimia tullaan näkemään lähitulevaisuudessa, koska se asettaa samantasoisia taloudellisia sanktioita organisaatioille kuin tietosuojadirektiivi GDPR. Katsauksen ensimmäisessä osassa tarkastellaan näiden direktiivien olemusta ja vaikutusta suomalaiseen kyberturvallisuuskenttään.

Tällä vuosituhannella Irlantiin on syntynyt Euroopan suurin datakeskusten keskittymä. Erityisesti amerikkalaiset IT-jätit ovat kilvan rakentaneet datakeskuksia Irlantiin lähinnä verotuksellisista syistä. Näihin keskuksiin on talletettuna esimerkiksi erilaisten somepalvelujen keräämät henkilötiedot. Datakeskuksen turvallisuudesta vastaa viime kädessä niiden omistaja, mutta ympäristölläkin on vaikutusta turvallisuuteen. Irlanti ei ole EU:n kärjessä kyberturvallisuuden tasossa, mutta tarjoaa kuitenkin kohtuullisen matalan riskin kyberympäristön datakeskuksille.

Hyökkäys on paras puolustus myös kybersodankäynnissä. Yhdysvaltojen johdolla useat maat muuttavat kybersodankäynnin doktriinia entistä hyökkäyksellisempään suuntaan. Katsauksen kolmannessa osassa valotetaan Yhdysvaltojen uuden kyberturvallisuusstrategian linjauksia sekä NATOn suunnitelmia tällä alueella.

Tekoälyä on pidetty yhtenä ratkaisevasta teknologiasta suurvaltojen välisessä poliittisessa, taloudellisessa ja sotilaallisessa kilpailussa. Yhdysvallat johtaa globaalia kilpailua ja Kiina seuraa toisena. Tekoäly on saavuttamassa maturiteettiasteen, jossa käytännön palveluja on mahdollista kehittää ja tarjota suurelle yleisölle. Samalla tekoälyteknologian erityisasema vähitellen sulautuu muiden teknologioiden joukkoon. Maailma kuitenkin odottaa vielä uusia, käänteentekeviä innovaatioita, mitä tämä teknologia-alusta mahdollistaa.

NIS2 JA CER – KOHTI PAREMPAA KYBERTURVAA JA RESILIENSSIÄ

// Timo Rinne

1. NIS2- ja CER-direktiivit aktivoivat jälleen EU-maiden kyberturvatalkoita. NIS2-direktiiviin on sisäänrakennettu GDPR-tasoinen sanktiojärjestelmä, joka on tärkeä tekijä konkreettisten parannusten vauhdittamiseksi.
2. NIS2- ja CER- direktiivit laajentavat kriittisen infrastruktuurin käsitettä useille uusille toimialoille. Lisäksi NIS2 on edeltäjäänsä paljon kattavampi vaatimuskokonaisuus ja tulee koskettamaan merkittävää osaa keskisuurista eli yli 250 henkilöä työllistävistä yrityksistä.
3. Uudet direktiivit hämmentävät helposti jo muutenkin monitahoista kyberturvallisuuden vaatimuskenttää. Vaarana on, että vaatimuksia luetaan liian teoreettisesti, olennaiset asiat hukkuvat ja suhteellisuuden taju katoaa. Vaikka standardeja ja direktiivejä on paljon, ne kaikki sisältävät samoja asioita eri näkökulmista painotettuina. Standardien ja direktiivien väliset suhteet on hyvä ymmärtää, jolloin parhaimmillaan voidaan edistää samalla työpanoksella usean kyberturvallisuuden vaatimusmäärittelyn.

EU:n kyberturvallisuusdirektiivi eli NIS2-direktiivi (Network Information Security 2) julkaistiin viime vuoden lopulla. Uusi direktiivi korvaa aiemman verkko- ja tietoturvadirektiivin ensimmäisen versio, joka on ollut voimassa noin viisi vuotta. Muiden direktiivien tapaan NIS2:n velvoitteet tuodaan osaksi kansallista lainsäädäntöä. Liikenne- ja viestintäministeriö on tämän vuoden alussa käynnistänyt toimeenpanohankkeen kansallisen lainsäädännön luomiseksi. Tämä työ on tarkoitus saada valmiiksi vuoden 2024 lopulla.

NIS2:n tarkoitus on tuoda kyberturvallisuusvaatimukset ajan tasalle ja korjata alkuperäisen direktiivin tehottomuusongelmia. Tehottomuus on ilmennyt erityisesti siten, että direktiivin velvoitteita on toimeenpantu ja valvottu hyvin kirjavasti Euroopan eri maissa. Tilanne on EU:n direktiiveille tyypillinen. Jotkut maat noudattavat vaatimuksia pilkulleen ja toiset tekevät omia priorisointejaan. Seurauksena on hyvin kirjava kyberturvallisuuden taso eri maissa, mikä ei edistä EU:n yhteistä pyrkimystä parempaan kyberturvallisuuden tasoon ja maiden resilienssiin.

Uusi direktiivi tuo kyberturvallisuuden parantamiseksi useita uusia velvoitteita. NIS2-direktiivi on huomattavasti kattavampi kuin entinen direktiivi ja sen piiriin kuuluu aiempaa useampia toimialoja sekä näiden piirissä olevia organisaatioita ja yrityksiä. Uusi direktiivi laajentaa yhteiskunnan kriittisten toimialojen valikoimaa ja asettaa näille kyberturvallisuuden uusia velvoitteita. Uusia direktiivin piiriin kuuluvia toimialoja ovat esimerkiksi jätevesihuolto ja avaruus. NIS2 koskee automaattisesti kaikkia keskisuuria eli yli 250 henkilöä työllistäviä yrityksiä, jotka toimivat kriittisillä toimialoilla.

NIS2-direktiivi jakaa kriittisillä toimialoilla toimivat yritykset ja organisaatiot keskeisiin ja tärkeisiin toimijoihin, joihin kohdistetaan erilaisia valvontatoimenpiteitä. Keskeisiä toimijoita valvotaan ennen toiminnan aloitusta tehtävillä valmiustarkastuksilla tai auditoinneilla. Tärkeitä toimijoita valvotaan jälkikäteen tehtävien tarkastusten avulla.

Velvoitteet voidaan jakaa karkeasti hallintatoimenpiteisiin ja raportointivelvoitteisiin. Hallintatoimenpiteet keskittyvät riskienhallintaan, mutta sisältävät käytännössä kaikki kyberturvallisuuden johtamisen ja hallinnon

perusvaatimukset. Raportointivelvollisuus sisältää GDPR:n tapaan aikarajat poikkeamien ilmoittamisesta viranomaiselle. Poikkeamista pitää antaa ennakkovaroitus 24 tunnin kuluessa ja tarkennettava tietoja 72 tunnin sisällä poikkeaman havaitsemisesta.

Kyberturvallisuuden hallintatoimien tai raportointivelvoitteiden laiminlyönnistä on asetettu GDPR-tasoa vastaavat sanktiot. Tämä tarkoittaa keskeisille toimijoille enintään 10 miljoonan euron tai 2% liikevaihdosta määritettyä sakkoa. Tärkeille toimijoille vastaavat luvut ovat 7 miljoonaa euroa ja 1,4% liikevaihdosta.

Toteutuneista GDPR-sakoista ei ole kovin paljon uutisoitu eikä niitä lukumääräisesti ole paljon määrättykään. Helmikuun loppuun 2023 mennessä Tietosuojavaltuutettu on määrännyt 17 hallinnollista sanktiota. Suurin tähänastinen sanktio määrättiin joulukuussa ruotsalaisen perintäkonsernin Alektumin Suomen yhtiölle. Sen suurus oli 750.000 euroa ja syynä oli yhtiön välinpitämätön suhtautuminen yksityishenkilöiden tietopyyntöihin. Toiseksi suurimman sakon on saanut Vastaamo (608.000 eur) ja kolmantena listalla on Viking Line (230.000 eur).

GDPR:n tapauksessa korkeiden hallinnollisten sanktioiden pelote on toiminut halutulla tavalla. Organisaatiot ja yritykset kasvattivat turvallisuusbudjettejaan parantaakseen tietosuojan tasoa ja useimmissa organisaatioissa käynnistettiin jonkunlainen tietosuojaprojekti. Tietosuojaan kohdistuva paine synnytti tietosuojaan liittyvää uutta liiketoimintaa esimerkiksi konsultointipalvelujen ja ohjelmistokehityksen alueilla. Lopputuloksena sekä eurooppalaiset että Eurooppaan palvelujaan tarjoavat yritykset paransivat aidosti henkilötietojen käsittelyn laatua ja turvallisuutta.

Samalla konstilla yritetään nyt korjata ensimmäisen NIS-direktiivin kokemaa tehottomuutta kyberturvallisuuden alueella. Kaikki Euroopan maat tulee saada mukaan kyberturvallisuuden talkoisiin. Asia on merkittävä Euroopan turvallisuuspoliittisen tilanteen vuoksi, joten kaikkien maiden tulee saada kyberturvallisuuden tilansa hyvälle tasolle.

NIS2:n sanktiopelotteella on kahdenlainen vaikutus. Toisaalta se pakottaa yritysten johdon suhtautumaan kyberturvallisuuteen tosissaan ja varmistamaan, että kyberturvallisuuden kehittämiseen on varattu tarvittavat resurssit. Toinen puoli on GDPR:stä tuttu suhteellisuuden tajun menetys, varsinkin, jos NIS2-vaatimuksia tulkitaan liian teoreettisesti ja kaikki riskit yritetään täydellisesti poistaa. NIS2:n implementointi käytäntöön edellyttää kokemusta turvakontrollien mitoituksesta oikein sekä kykyä priorisoida eteen tulevia kehityskohteita. Muutoin on vaarana, että ”ammutaan kärpästä tykillä” ja kyberturvatiimi ajetaan näännyksiin sellaisten asioiden korjaamisessa, joilla ei ole käytännön kannalta merkitystä.

Toinen kyberturvallisuutta ja huoltovarmuutta käsittelevä, käsittelynsä loppupuolella oleva EU-direktiivi on nimeltään CER (Critical Entities Resilience). CER-direktiivin tarkoituksena on yhtenäistää ja vahvistaa EU-maiden kriittisten toimijoiden resilienssin ja varautumisen käytäntöjä. Kriittinen infrastruktuuri on EU:ssa todettu suurelta osin haavoittuvaksi ja CER-direktiivin tarkoitus on yhdessä NIS2-direktiivin kanssa parantaa yhteiskunnan häiriönsietokykyä.

Kriittinen infrastruktuuri on ollut perinteinen kyberrikollisten ja valtiollisten kybertoimijoiden lempikohde. Useat kriittisen infrastruktuurin alueet ovat kyberturvallisuuden näkökulmasta haavoittuvia, kukin omalla tavallaan. Esimerkiksi energiantuotannossa ja vesihuollossa käytetään paljon vanhoja teollisuuden järjestelmiä, jotka on alun perin rakennettu suljetuiksi, mutta jotka on nykyisin avattu julkisiin verkkoihin etähallintavaatimusten myötä. Tällä tavalla alun perin huonosti suojatut järjestelmät ovat tulleet avoimesti kyberrikollisten pelikentälle. Pankki- ja finanssimarkkinoiden IT-infrastruktuuri on rakennettu nykyaikaisemman teknologian varaan, mutta näitäkin on onnistuttu vahingoittamaan.

Sekä NIS2 että CER tuovat jälleen painetta organisaatioille kyberturvallisuuden parantamiseen. GDPR ja viimeisimmäksi myös julkishallinnon toimijoihin kohdistuva Tiedonhallintalaki ovat kasvattaneet kyberturvallisuuden budjetteja ja pidentäneet kyberturva-ammattilaisten työpäivää. NIS2:n ja CERin lisäksi keskusteluissa vilisee useita muitakin kyberturvallisuuteen liittyviä tai sitä sivuavia vaatimuksia, jolloin riski hukkua erilaisten vaatimusten viidakkoon kasvaa.

Vaikka keskusteluissa esiintyy useita erilaisia kyberturvallisuuden vaatimuksia, ne eivät ole toisistaan täysin erilaisia, vaan kaikkien tavoitteena on parantaa kyberturvallisuutta erilaisista näkökulmista. Standardien ja direktiivien väliset suhteet on hyvä ymmärtää, jolloin parhaimmillaan voidaan edistää samalla työpanoksella usean kyberturvallisuuden vaatimusmäärittelyn tavoitteita. Kokonaisuuden hahmottaminen edellyttää kuitenkin useamman ministeriön työn seurantaa, sillä valmistelutyöt kyberturvallisuuden eri vaatimusmäärittelyiden osalta on jaettu jokainen eri ministeriöön. NIS2 kuuluu liikenne- ja viestintäministeriölle, CER sisäministeriölle ja Tiedonhallintalaki valtiovarainministeriölle. Kokonaisuus on hallittavissa, vaikkakin kyberturvallisuuteen liittyvien parannushankkeiden keskitetty johtaminen ja koordinointi voisi helpottaa asiaa. ■

Lähteet sivulla 32

MAA-ANALYYSI: IRLANTI

// Timo Rinne

1. Amerikkalaiset IT-jätit kuten Google, Microsoft, Amazon ja Apple ovat luoneet Irlantiin Euroopan suurimman datakeskusten keskittymän. Näissä datakeskuksissa on talletettuna myös valtavat määrät henkilötietoja. Datakeskusten omistajilla on miljardiluokan vuosibudjetit kyberturvallisuuden varmistamiseen.

2. Irlannin kyberturvallisuuden taso on Euroopan mittakaavassa keskitason alapuolella. Irlanti on ITU:n globaalin kyberturvallisuusindeksin Euroopan listalla sijalla 28. Suurimmat puutteet ovat kyberturvallisuuden yhteistyössä eri organisaatioiden ja yritysten välillä. Irlanti on vuonna 2021 perustanut kansallisen kyberturvallisuuden kehittämiskeskuksen parantamaan yhteistyötä.

3. Irlannin kyberturvallisuutta johtaa kansallinen kyberturvallisuuskeskus. Kybersodankäynnin joukot on sijoitettu Irlannin armeijan viestiaselajiin. NATO-yhteistyö antaa kybersodankäynnin kehittämiselle hyvät lähtökohdat myös tulevaisuudessa.

4. Irlanti on hieman Euroopan keskitason alapuolella kyberrikollisuuden osalta. Vuonna 2021 joka kolmas PK-yritys raportoi joutuneensa jonkinlaisen kyberhyökkäyksen tai -rikollisuuden tai sellaisen yrityksen kohteeksi. Datakeskusten turvallisuus ei kuitenkaan ole sen vuoksi erityisen uhattuna.

Tällä vuosituhannella Irlantiin on syntynyt Euroopan suurin datakeskusten keskittymä. Erityisesti amerikkalaiset IT-jätit ovat kilvan rakentaneet datakeskuksia Irlantiin. Irlannin suosion syiksi on selitetty osaavaa IT-työvoimaa, energiakustannuksia säästävää viileää ilmastoa ja tuulivoimaa, maantieteellistä läheisyyttä Amerikan mantereelle sekä ennen kaikkea verotuksellisia ja taloudellisia syitä. Irlannin yritysverotus on ollut viime vuosina EU-tason matalimpia. Irlannin yritysverotuksen perusprosentti on 12,5, jonka päälle ulkomaisille yrityksille lisätään muutaman prosentin preemio liiketoiminnan laajuudesta ja luonteesta riippuen. Kokonaisprosentti jää kuitenkin selvästi alle kahdenkymmenen.

Amerikkalaisten IT-jättien kiinnostus siirtää datakeskustoimintojaan Eurooppaan kiihtyi viimeistään GDPR-direktiivin myötä 2010-luvun loppupuolella. GDPR vaikeutti merkittävästi ei-Eurooppalaisten palveluntarjoajien operaatioita vaatimalla, että henkilötietojen tulee lähtökohtaisesti olla talletettuna EU:n maaperällä. Henkilötietojen talletus ja käsittely EU:n ulkopuolella on mahdollista, mutta vain erityissopimuksilla ja -järjestelyillä. Näin käytännössä kaikki amerikkalaiset datajätit kuten Microsoft, Google, Meta/Facebook, Amazon ja Apple perustivat datakeskuksiaan Irlantiin. Nykyisin datakeskustoiminta on niin laajaa, että niiden sähkönkulutus ja sen myötä ympäristövaikutukset ovat nousseet huolen aiheeksi.

Jos Irlantiin on talletettu Euroopan suurimmat henkilötietovarastot, onko meidän syytä olla huolissaan tietovarastojen kyberturvallisuudesta? Datakeskusten kyberturvallisuus on ensi sijassa niiden omistajien vastuulla ja hallinnassa. Kaikki suuret IT-yhtiöt ovat pääsääntöisesti toteuttaneet palveluidensa kyberturvallisuuden laadukkaasti. Tämän mahdollistavat ennen näkemättömät kyberturvallisuuden budjetit. Amazon, Apple, Google,

Microsoft ja IBM kertoivat viime vuonna käyttävänsä yhteensä noin 30 miljardia dollaria seuraavien viiden vuoden aikana kyberturvallisuuden ylläpitoon ja kehittämiseen. Yhtiötä kohden tämä tarkoittaa keskimäärin reilun miljardin dollarin vuosibudjettia.

Vaikka datakeskusten kyberturvallisuuden toteutus on pitkälti omistajiensa käsissä, myös ympäristöllä on vaikutusta. Kyberrikollisuus rehottaa yleensä siellä, missä sen on helpointa toimia ja missä kyberturvallisuuden yleinen taso ei ole korkealla. Irlanti sijoittuu ITU:n kansainvälisessä kyberturvallisuusindeksissä vasta sijalle 46 ja Euroopassakin sijalle 28.

Mihin Irlannin vaatimaton suorituskyky kyberturvallisuudessa perustuu? Kyberturvaindeksi mittaa maan kypsyyttä lainsäädännön, organisoinnin, yhteistyön, osaamisen ja teknisten valmiuksien perusteella. Irlanti saa lähes täydet arvosanat lainsäädännön ja teknisen kyberturvallisuuden osalta. Irlannin kyberlainsäädäntö perustuu EU:n direktiiveihin, jotka Irlanti on vienyt kansalliseen lainsäädäntöön tehokkaasti ja viivyttelemättä. Teknisen kyberturvallisuuden osa-alue kohdistuu kansallisen kyberturvallisuuskeskuksen toimintaan ja tälläkin osa-alueella Irlanti suoriutuu moitteetta monen muun EU-maan lisäksi.

Organisoinnin osa-alueen keskiössä on kansallinen kyberturvallisuusstrategia ja kyberturvallisuuden johtaminen. Edelleen Irlanti saa eurooppalaisittain hyvät arvosanat tästä osa-alueesta. Kyberturvallisuuden osaamisessa Irlanti on korkeintaan EU:n keskitasoa. Osaamisessa mitataan maan aktiivisuutta kyberturvallisuuden koulutuksen ja eri väestönryhmille suunnattujen tiedotuskampanjoiden avulla. Irlannissa on parannettavaa kansallisen kyberturvallisuustietoisuuden ja kyberhygienian alueilla.

Huonoimman arvosanan Irlanti saa kyberturvallisuuteen liittyvän yhteistyön alueella. Tällä osa-alueella tarkastellaan julkisen ja yksityisen sektorin välisiä yhteistyöhankkeita, julkishallinnon eri organisaatioiden välistä yhteistoimintaa sekä kansainvälisiä yhteistyö- ja tiedonvaihtosopimuksia. Irlanti onkin perustanut vuonna 2021 kansallisen kyberturvallisuuden kehittämiskeskuksen parantamaan tämän osa-alueen suorituskykyä.

Irlannin kybertoimintaa johtaa ja koordinoi kansallinen kyberturvallisuuskeskus (National Cyber Security Centre). Keskus toimii ympäristö- ja viestintäministeriön (Ministry for the Environment, Climate and Communications) alaisuudessa. Keskuksen vastuulla on pääasiassa julkishallinnon tietoverkkojen turvaaminen, yksityissektorin ja kansalaisten kyberkoulutus ja neuvonta, kybertilannekuvan ylläpito ja valvonta sekä häiriötilanteiden ratkaiseminen eli niin sanotto CSIRT-toiminta (Computer Security Incident Response Team).

Irlannin kyberturvallisuuskeskus tekee läheistä yhteistyötä Irlannin puolustusvoimien ja erityisesti viestiaselajin kanssa. Kybersodankäynnin joukot ja osaaminen on keskitetty Irlannin armeijan CIS-joukkoihin (Communications & Information Services Corps). Kyberjoukkojen lisäksi CIS vastaa sotilasviestiliikenteestä sekä teknisestä sotilastiedustelusta.

> **Amerikkalaiset IT-jätit kuten Google, Microsoft, Amazon ja Apple ovat luoneet Irlantiin Euroopan suurimman datakeskusten keskittymän. Datakeskusten omistajilla on miljardiluokan vuosibudjetit kyberturvallisuuden varmistamiseen.**

CIS:n kybersotilaat saavat koulutuksensa armeijan omissa koulutuslaitoksissa ja irlantilaisissa tekniikan alan yliopistoissa. Carlowin teknilliseen yliopistoon on perustettu erityisiä kyberturvallisuuteen ja sotilasteknologiaan keskittyviä opintolinjoja. Dublinin yliopistossa toimii kyberturvallisuuden tutkimuskeskus (Centre for Cybersecurity and Cybercrime Investigation), joka toimii läheisessä yhteistyössä CIS-joukkojen, Irlannin poliisin sekä kyberturvallisuuskeskuksen kanssa koulutus- ja tutkimustoiminnassa.

Irlanti on hieman Euroopan keskitason alapuolella kyberrikollisuuden osalta. Vuonna 2021 joka kolmas PK-yritys raportoi joutuneensa jonkinlaisen kyberhyökkäyksen tai -rikollisuuden tai sellaisen yrityksen kohteeksi. Euroopan keskiarvo on 28%. Noin 12% kiristyshaittaohjelmien kohteeksi joutuneista PK-yrityksistä oli maksanut lunnaita. Luku on kaksinkertainen Euroopan keskiarvoon verrattuna.

Irlannin kyberrikollisuuden historian kuuluisin tapaus on toukokuussa 2021 maan terveydenhuollon tietojärjestelmiin kohdistunut, kiristyshaittaohjelman avulla tehty hyökkäys. Irlannin terveydenhuollon tietojärjestelmät joutuivat välittömästi kaaokseen ja paperipohjaisia varamenetelmiä otettiin käyttöön. Tietojärjestelmien häirinnän lisäksi potilastietoja anastettiin ja julkaistiin verkossa. Tapauksen selvittelyyn ja tietojärjestelmien toipumiseen osallistuivat myös Irlannin armeijan CIS-joukot ja se kutsui riveihinsä myös lukuisia reserviläisiä tilanteen ratkaisemiseksi.

Irlannin kyberturvallisuuden tulevaisuuden kehityksellä on tukenaan EU:n ja NATOn tuki ja resurssit. EU-lainsäädäntö on maailman edistyksellisimpiä ja direktiivien vaatimukset valuvat kansalliseen lainsäädäntöön nopeasti. Irlannin asevoimat tekevät tiivistä yhteistyötä NATOn kanssa, osallistuvat NATOn kybersotaharjoituksiin ja pysyvät NATO-yhteistyön avulla kehityksen mukana. Irlannissa esiintyy vakavaakin kyberrikollisuutta, mutta datakeskusten turvallisuus ei ole sen vuoksi erityisen uhattuna. ■

Lähteet sivulla 32

OFFENSIIVINEN KYBERPUOLUSTUS

// Timo Rinne

1. Yhdysvallat johtaa globaalia kehitystä hyökkäyksellisen kybertoiminnan alueella. Yhdysvaltojen uuden kyberturvallisuusstrategian mukaan kybervastustajien toimintakyvyn heikentäminen on yksi kyberpuolustuksen pääpilareita.

2. Defend forward -strategia sijoittuu aggressiivisen hyökkäyksen ja passiivisen puolustuksen välimaastoon. Strategian avulla kriittisimpiä kohteita vahvistetaan siten, että hyökkäyksen kustannukset ja kiinnijäämisen riski kasvavat ja hyökkääjä mahdollisesti päättää luopua hyökkäyksestä.

3. NATO-maiden valmiudet kyberaseiden valmistamiseen ja kyberhyökkäysten toteutukseen vaihtelevat suuresti. NATO on luonut oman strategian kyberhyökkäysten toteutukselle, joka mahdollistaa jäsenmaiden itsenäisen toiminnan NATOn sisällä.

4. Kyberaseita ja kyberhyökkäyksiä on käytetty jo pitkään, ja ne ovat tulossa entistä näkyvämmin esille kyberturvallisuuden strategioihin. Tulevaisuudessa kyberpuolustusta ei voi tehokkaasti toteuttaa ilman kykyä hyökkäykselliseen toimintaan. Kehityskulku asettaa paineita niille maille, joilla hyökkäyksellisen toiminnan kehitys on vasta alkumetreillä. Esimerkiksi NATO-maista vasta noin puolella on kykyjä ja resursseja hyökkäykselliseen kybertoimintaan.

Presidentti Bidenin hallinto julkaisi Yhdysvaltojen uuden kyberturvallisuusstrategian maaliskuun alussa. Amerikkalaiseen tyyliin strategia on rakennettu muutaman ”pilarin” varaan, jotka määrittelevät strategian korkean tason tavoitteet ja periaatteet. Kyberturvallisuusstrategiassa on viisi pilaria, joista järjestyksessä toinen vauhdittaa amerikkalaisen kyberpuolustuksen kehittämistä nykyistä enemmän hyökkäykselliseen suuntaan.

Yhdysvallat nimeää uudessa strategiassaan pahimmat kybervihollisensa, joita ovat Kiina, Venäjä, Iran ja Pohjois-Korea. Nimettyjen valtioiden lisäksi Yhdysvaltojen vihollisena mainitaan yleisesti kyberrikolliset. Strategian mukaan Kiinan toiminta on pääasiassa kybervakoilua oman tieteellisen, taloudellisen ja ideologisen vaikutusvallan kasvattamiseksi globaalisti. Venäjän tavoitteena on häiritä länsivaltojen kriittistä infrastruktuuria, käyttää Internetiä disinformaation levittämiseen sekä tukea kyberhyökkäyksillä sen sotilaallista toimintaa tällä hetkellä Ukrainaa vastaan. Iranilla on pääasiassa Lähi-Idän alueelle kohdistuva maantieteellinen fokus Yhdysvaltojen ja sen kumppaneiden häiritsemiseksi kyberavaruuden kautta. Pohjois-Korean pääasiallinen tarkoitus on kerätä varoja maalle ja erityisesti sen ydinasehankkeille kyberrikollisuuden avulla.

Kyberstrategian toisen pilarin mukaan Yhdysvallat taistelee kybervihollisiaan vastaan hyökkäyksellisin keinoin. ”Disrupt and Dismantle Threat Actors” -pilarin mukaan Yhdysvallat pyrkii aktiivisesti heikentämään vihollistensa kybertoimintakykyä. Toimenpiteisiin voidaan lukea varsinaisten kyberhyökkäysten lisäksi diplomaattisia ja taloudellisia toimia, informaatiovaikuttamista sekä sotilaallista voimaa. Strategian mukaan on siis mahdollista, että Yhdysvallat voi jopa tuhota fyysisesti vastustajan kybertoimintaan liittyviä elementtejä.

Hyökkäyksellinen kybersodankäynti ei ole Yhdysvaltojen doktriinissa uusi asia. Kehitys alkoi jo 2010-luvun alussa, kun presidentti Obaman hallinto määritteli silloin vielä monimutkaisen prosessin, jonka tuloksena kyberhyökkäyksiä voi suunnata toisia valtioita tai kyberrikollisia kohtaan. Kyberhyökkäysten kynnys on madaltunut vuosi vuodelta ja hyökkäyksen aloittaminen helpottui merkittävästi vuonna 2018 presidentti Trumpin hallinnon määriteltyä entistä nopeamman prosessin hyökkäyksen käynnistämiseksi.

Haittaohjelmat ovat kybersodankäynnin perustyökaluja. Siinä missä Yhdysvaltojen viholliset käyttävät esteettä APT-ryhmiä eli kyberrikollisia aseiden valmistamiseen, NSA ja nykyisin myös Yhdysvaltojen armeijan Cybercommand -yksikkö toimivat Yhdysvaltojen kyberasetehtaina.

Kybersodankäyntiin valmistetut haittaohjelmat perustuvat lähes poikkeuksetta nollapäivähaavoittuvuuksiin, joten niiden valmistaminen edellyttää paljon aikaa ja resursseja.

Yhdysvaltojen hyökkäyksellinen kyberstrategia on synnyttänyt myös konflikteja ennalta ehkäisevän strategian ”defend forward”. Käsite on esitetty ensimmäisen kerran Yhdysvaltojen kybersodankäynnin keskuksen US Cybercommandin kirjoituksissa jo vuonna 2018. Defend forward tarkoittaa kybervihollisen ja kyberhyökkäysten torjuntaa jo ennen niiden realisoitumista, eikä vasta sitten, kun hyökkäys on havaittu sen kohteessa. Konsepti on muuttanut kyberpuolustusta radikaalisti reaktiivisesta proaktiiviseen suuntaan.

Defend forward -konseptin tavoitteena on muuttaa hyökkääjän käyttäytymistä ja aikeita siten, että se mahdollisesti luopuu kyberhyökkäyksestä jo sen suunnitteluvaiheessa. Käytännössä tämä tavoite voidaan saavuttaa erilaisilla ennakoivilla vastatoimenpiteillä, jotka kaikki edellyttävät tehokasta kybertiedustelua ja hyökkääjän aikeiden selvittämistä.

Kun on tehty havainto mahdollisesta vihollisen suunnittelemasta kyberhyökkäyksestä ja ymmärretty sen kohde, voidaan kohteen suojausta vahvistaa ja hyökkääjän kiinnijäämisriskiä lisätä merkittävästi. Toimenpiteen onnistuessa hyökkääjä ei enää näe kohdetta helppona maalina, vaan ymmärtää, että operaation suorittamiseksi tarvitaan enemmän aikaa ja resursseja, jolloin hyökkääjä perääntyy tai joutuu ainakin muuttamaan suunnitelmiaan.

Toinen mahdollisuus on heikentää kyberhyökkäyksestä saatavaa etua. Yhdysvaltojen kyberturvallisuusstrategiassa on erityisesti mainittu talousrikollisuuden torjunnan toimenpiteet kryptovaluuttojen käytön vaikeuttamiseksi. Kryptovaluutat kuten Bitcoin, ovat kyberrikollisten käytännössä ainoa mahdollisuus muuttaa vaikkapa ransomware-hyökkäyksen tulos taloudelliseksi tuotoksi. Kybervaluuttojen käytön vaikeuttamisella pyritään ransomware-hyökkäysten ennalta ehkäisyyn ja rikollisten kiinnijäämisriskin nostamiseksi.

Myös NATO on muuttamassa kyberpuolustustaan entistä enemmän hyökkäykselliseen suuntaan. Kybersodankäynti itsessään on NATOn toiminnassa vielä kehitysvaiheessa. NATO perusti vuonna 2008 Tallinnaan Naton kyberpuolustuksen osaamiskeskuksen ja on tutkinut kybersodankäyntiä jo pitkään. NATO tunnusti vasta vuonna 2016 yleiskokouksessaan kyberavaruuden yhdeksi sodankäynnin toimintaympäristöksi maan, ilman ja meren lisäksi. Pian tämän jälkeen NATO perusti kyberoperaatiokeskuksen CyOC:n (Cyber Operations Center) koordinoimaan sen kyberpuolustusta.

Puolustuksellisessa kybersodankäynnissä NATO-maat tekevät tiivistä yhteistyötä, jakavat toisilleen uhkatiedustelun tilannekuvaa ja osallistuvat kyberpuolustukseen NATOn kyberoperaatiokeskuksen kautta. Kyberhyökkäysten toteuttamisen osalta yhteistyö tai koordinointi ei ole näin tiivistä. NATO-maiden valmiudet kyberaseiden valmistamiseen ja hyökkäysten toteutukseen vaihtelevat suuresti. 2020-luvun alussa kolmestakymmenestä NATO-maasta vain puolet ilmoitti omaavansa hyökkäyksellisiä kyberkyvykkyyksiä tai olevansa kehittämässä sellaisia (OCO, Offensive Cyberspace Operations). Kyberhyökkäyksiä varten NATO onkin kehittänyt jäsenmaiden itsenäistä toimintaa korostavan strategian, joka tunnetaan nimellä SCEPVA (Sovereign Cyber Effects Provided Voluntarily by Allies).

SCEPVA-strategia antaa jäsenmaille mahdollisuuden kehittää ja käyttää itsenäisesti hyökkäyksellisiä kyberaseita, esimerkiksi haittaohjelmia. Strategia antaa NATO-maalle kolme toimintavaihtoehtoa kyberhyökkäyksen toteutukseen; 1) jakaa tietoa haittaohjelmasta ja sen vaikutuksesta NATO-maiden kesken ennen hyökkäystä, 2) ilmoittaa NATOlle etukäteen kyberhyökkäyksestä paljastamatta kyberaseen yksityiskohtia tai 3) toteuttaa kyberhyökkäys täysin itsenäisesti ja ilman etukäteisinformaatiota NATOlle.

SCEPVA-strategian taustalla on useita kybersodankäyntiin liittyviä erityispiirteitä. Kyberaseet ovat kertakäyttöisiä eli samaan haavoittuvuuteen perustuvaa kyberasetta ei voida toista kertaa käyttää, koska kohteen suojausohjelmat päivitetään nopeasti haavoittuvuuden löydyttyä. Kyberaseen kehittänyt jäsenmaa haluaa useimmiten valita käyttökohteen itsenäisesti eikä luovuttaa kyberasetta tai tarkkaa tietoa sen toimintaperiaatteista NATOn koordinoitavaksi.

Haittaohjelmien kehitystyö ja näiden ominaisuudet on pidettävä tarkasti salassa ennen hyökkäyksen toteutusta. Pahimmassa tapauksessa paljastunutta haittaohjelmakoodia voidaan käyttää sen laatijaa vastaan, kuten usein on ennemmin tai myöhemmin haittaohjelman paljastumisen jälkeen tapahtunut. Kolmas erityispiirre liittyy NATO-maiden kyvykkyyseroihin kyberaseiden kehityksessä. Noin puolet NATO-maista pystyy kehittämään kyberaseita ja näidenkin sisällä on suuri osaamisen kirjo, eikä tätä osaamista haluta välttämättä aktiivisesti jakaa muiden jäsenmaiden kanssa.

Kyberpuolustus on voimakkaassa muutoksessa hyökkäykselliseen suuntaan. Yhdysvallat ja sen keskeisimmät vastustajat ovat kehittäneet ja käyttäneet kyberaseita jo vuosia, mutta niiden käyttö tuodaan nykyisin entistä näkyvämmin mukaan kyberturvallisuuden strategioihin. Aggressiivisen hyökkäystoiminnan lisäksi on kehitetty ennalta ehkäiseviä strategioita kuten Defend forward, jota on myös sovellettu yritysmaailmaan. NATO-maiden kyberkyvykkyyksien tasoittuessa, myös puolustusliiton hyökkäyksellistä kybertoimintaa voidaan koordinoida tehokkaammin. ■

Lähteet sivulla 32

KANSAINVÄLINEN KILPAILU TEKOÄLYTEKNOLOGIASTA

// Timo Rinne

1. Kyberavaruus on yksi sodankäynnin domain eli toimintaympäristö maa-, meri-, ilma- ja avaruusympäristöjen lisäksi. Kybersodankäyntiin kehitetyt aseet ovat pääasiassa kohdennettuja haittaohjelmia.

2. Kyberaseet ja tavanomaiset aseet eroavat toisistaan monin tavoin. Kyberaseet pidetään salaisina aina niiden käyttöön asti, jotta niiden käyttöperiaatteet ja ominaisuudet eivät paljastuisi kohteelle. Tavanomaisilla aseilla pyritään luomaan niiden julkisuuden kautta pelotevaikutus, jotta varsinainen sotatilanne olisi mahdollista välttää.

3. Vastapuolen kybersodankäynnin kyvykkyyttä on vaikea selvittää. Kybertiedustelun tulee tapahtua mahdollisen kyberhyökkäyksen kohteen ympäristössä, jotta hyökkääjän valmistelut ja mahdollinen kyberaseen testaus voidaan havaita. Yhdysvallat on luonut kohteessa tapahtuvalle kybertiedustelulle Hunt Forward -nimisen konseptin, jonka avulla se on onnistunut selvittämään esimerkiksi Kiinan ja Venäjän kyberaseiden ominaisuuksia.

4. Kyberrikolliset ja -terroristit hyödyntävät tehokkaasti käytettyjä kyberaseita. Kerran käytetty ja sen myötä paljastunut kyberase voidaan hyödyntää heikommin. puolustettuja kohteita vastaan joko sellaisenaan tai muunneltuna versiona.

Tekoälysovellukset ovat viime kuukausina tehneet rynnistyksen kuluttajien ulottuville. ChatGTP on ihastuttanut kokeilijoitaan ratkaisemalla monimutkaisiakin tehtäviä ja vaikka kirjoittamalla runoja halutusta aiheesta tai kokoamalla vakuuttavan ansioluettelon työnhakua varten. ChatGPT on ensimmäisiä kuluttajien käyttöön toteutettuja ja helpon käyttöliittymän omaavia tekoälypalveluja.

Tekoäly on kuitenkin toiminut kuluttajien parissa taustalla jo vuosia. Erityisesti mobiililaitteiden ja -palvelujen valmistajat ovat käyttäneet tekoälyalgoritmeja toimintoihin, jotka parantavat näiden suorituskykyä kuluttajan sitä itse tiedostamatta. Puhelinten kameroiden hahmontunnistus ja automaattitarkennukset ja -valotukset toimivat tekoälyn avulla. Käyttäjä opettaa itse tekoälysovelluksia tiedostamattaan some-palveluja käyttämällä, jolloin nämä tuottavat käyttäjälle esimerkiksi paremmin kohdennettua sisältöä.

Myös monet julkishallinnon palvelut sekä liike-elämä hyötyvät tekoälyn käytöstä. Röntgenkameran ohjelmisto oppii tunnistamaan syöpäkudoksia automaattisesti, maatalouden tuotantoa voidaan tehostaa ennustamalla sääilmiöiden vaikutuksia ja kuljetuspalvelujen tehokkuutta voidaan parantaa optimoimalla reitit liikennemäärien ja keliolosuhteiden mukaan.

Tekoälylle voidaan delegoida automaattista päätöksentekoa monessa eri tilanteessa. Jos laadukas tekoälysovellus ilmaisee lopputuloksen olevan lähes varma, ei matalan riskin päätökseen kannata välttämättä tuhlata ihmisen harkinta-aikaa, vaan sovellus voi tehdä suoraan päätöksen. Tekoälyä voidaan soveltaa myös sotilaallisiin sovelluksiin nopeuttamaan tilanteenmukaista päätöksentekoa harkituissa tilanteissa.

Tekoälyteknologia on tärkeä tulevaisuuden mahdollistaja myös kyberturvallisuudessa sekä kyberhyökkäysten että -puolustuksen näkökulmasta. Tekoälyä voidaan käyttää kyberhyökkäyksiin lähinnä kolmella tavalla. Ensimmäinen on tekoälyn käyttö kohteen tiedusteluvaiheessa. Tekoälypohjainen OSINT-sovellus oppii kohteen kybersuojauksen käytännöt nopeasti. Esimerkiksi kuinka usein ja millä viiveellä järjestelmiä päivitetään, kohdejärjestelmän käyttöaste ja sen vaihtelut sekä käyttöoikeuksien muutosten ajoittuminen ovat tärkeitä tietoja kyberhyökkäyksen ajoittamisessa ja heikoimman kohteen löytämisessä.

Toinen keino on varustaa itse haittaohjelma tekoälyalgoritmilla, jolloin se kykenee kohdejärjestelmään pääsyn jälkeen oppimaan edellä kuvattuja asioita ja suorittamaan hyökkäyksen kaikkein otollisimpana hetkenä. Kolmas keino on manipuloida kohteessa olevia tekoälyjärjestelmiä niiden opetusvaiheessa. Tekoälyn toimivuus perustuu tällä hetkellä järjestelmän opettamiseen määritellyn datajoukon avulla. Jos hyökkääjä pääsee manipuloimaan järjestelmän opetukseen käytettävää dataa, voi hän saada kohteen tekoälyjärjestelmän toimimaan haluamallaan tavalla.

Kyberpuolustuksessa tekoälyä käytetään tietenkin päinvastoin, eli hyökkääjän toiminnan erityispiirteiden tunnistamiseen ja ennakointiin. Lisäksi tekoälyn avulla voidaan merkittävästi parantaa kyberturvallisuushälytysten luotettavuutta. Staattiset säännöt tuottavat usein merkittävän määrän vääriä hälytyksiä. Tekoälyn avulla voidaan oppia väärien hälytysten piirteitä ja nostaa esiin vain kaikkein tärkeimmät havainnot. Luonnollisen kielen käsittelyjärjestelmä (NLP, natural language processing) on tekoälyn osa-alue, jonka avulla voidaan ennustaa kyberhyökkäyksiä analysoimalla tekstiä ja siinä esiintyviä hyökkäystä edeltäviä ilmiöitä tai vaikkapa tunnetiloja.

Vuonna 2022 tekoälyteknologioiden ja -palvelujen kehittämiseen ja toteutukseen käytettiin globaalisti noin 430 miljardia dollaria. Varsinainen tekoälymarkkina, eli asiakkaiden investoinnit ja kulutus tekoälytoteutuksiin on tätä pienempi, hieman yli sata miljardia dollaria. Markkinoiden koko on noin puolet verrattuna globaaleihin kyberturvamarkkinoihin. Ala on siis vielä vahvasti tuotekehitysvaiheessa, mutta jo vuonna 2025, tekoälymarkkinoiden pelkän tuoton arvioidaan olevan sadan miljardin luokkaa.

Valtioiden tekoälykyvykkyyksien vertailuun on kehitetty erilaisia indeksejä. Yleensä tällaisten indeksien mittareina toimivat aiheeseen liittyvä lainsäädäntö, infrastruktuurin valmius, julkisen ja yksityisen sektorin investoinnit, teknologian käyttöaste sovelluksissa, tutkimus ja tuotekehityshankkeiden määrä jne. Useat toimijat IBM:stä Stanfordin yliopistoon ovat kehittäneet omia indeksejään maiden tekoälykyvykkyyksien arviointiin.

Yksi arvostetuimmista indekseistä on brittiläisen Tortoise Community -ajatushautomon Global AI Index. Sen mukaan ylivoimainen ykkönen on Yhdysvallat, yhtä selvä kakkonen Kiina ja kolmossijan tuntumassa hyvin lähekkäin toisiaan ovat Iso-Britannia, Kanada, Israel, Singapore ja Etelä-Korea. Suomi on kokonaistilastossa sijalla 13, heti perässä seuraa Tanska ja muista pohjoismaista Ruotsi on sijalla 19, Norja 25 ja Islanti 37.

Yhdysvaltojen paalupaikka on helppo ymmärtää. Maassa toimivien IT-jättiläisten voittokulku on luonut Yhdysvalloille toistaiseksi kiistämättömän aseman kaikessa IT-teknologiaan liittyvässä kehityksessä. Yhdysvalloilla on tällä hetkellä ylivoimainen johtoasema tutkimus- ja tuotekehitystoiminnassa sekä tekoälyn kaupallistamisessa. Myös suurin osa maailman tekoälyosaajista työskentelee tällä hetkellä Yhdysvalloissa. Yhdysvallat jää selvästi muuta maailmaa jälkeen tekoälyä säätelevien regulaatioiden valmiudessa, julkishallinnon strategioissa sekä kansan valmiuksissa ottaa teknologia hyötykäyttöön.

Kiinan kakkossija on yhtä selvä lähes kaikilla osa-alueilla. Se jopa ohittaa Yhdysvallat infrastruktuurin valmiudessa tekoälyn käyttöön. Tällä tarkoitetaan esimerkiksi tietoliikenneinfrastruktuurin ja erityisesti 5G-verkkojen kehitystä sekä tekoälyn tarvitseman laskentakapasiteetin levinneisyyttä supertietokoneiden ja näiden verkkojen muodossa. Tekoälyosaamisen alueella Kiina jää hieman yllättävästikin monen muun maan taakse. Sen sijaan Intia on tällä osa-alueella kakkosena heti Yhdysvaltojen jälkeen.

Mutta missä on Venäjä? Se löytyy kokonaistilastossa vasta sijalta 32. Sen sijoitus kaikilla osa-alueilla on kokonaissijoituksen mukainen, mutta Venäjä sijoittuu kuuden parhaan joukkoon valtionhallinnon strategioissa ja kehittämisohjelmissa. Venäjällä siis panostetaan tekoälyn tutkimukseen, tuotekehitykseen ja kaupallistamiseenkin, mutta tulokset ovat ainakin toistaiseksi jääneet selvästi jälkeen muista maailman suurvalloista, jos Venäjää voi enää sellaiseksi lukea.

Venäjän heikko tulos kansainvälisessä vertailussa ei kyberturvallisuuden osalta kerro kaikkea. Venäjän tekoälypanostukset ovat mitä ilmeisimmin keskittyneet erityisesti valtionhallinnon hankkeisiin ja sotilasteknologiaan, jolloin niiden valmius voi olla huomattavastikin korkeampi kuin mitä julkiset tilastot näyttävät. Venäjä myös tukeutuu tällä alueella Kiinaan, joka on sitä tukenut monella korkean teknologian alueella, esimerkiksi 5G-teknologian käyttöönotossa.

Autoritääristen valtioiden teknologisten kyvykkyyksien arviointi on yleensäkin ottaen haastavaa. Julkinen rahoitus ei ole avointa, valtio sääntelee tieteellistä julkaisutoimintaa eikä maan kärkiosaamista tuoda kaupallisiin sovelluksiin, vaan voimavarat keskitetään valtionhallinnon omiin tarkoituksiin. Näin ollen esimerkiksi Kiinassa ja Venäjällä kehitys voi olla pidemmällä kuin mitä julkiset lähteet antavat ymmärtää.

Autoritaaristen valtioiden suurin haaste tekoälyn kehityksessä on kuitenkin huippuasiantuntijoiden puute. Sekä Kiinassa että Venäjällä kyllä tuotetaan omia asiantuntijoita, mutta näiden valtioiden yhteiskuntajärjestys ja olosuhteet eivät houkuttele ulkomaisia huippuosaajia maahan muutoin kuin ehkä ideologisista syistä. Länsimainen, yksilön vapauksia korostava yhteiskunta ja mahdollisuus innovaatioiden kaupallistamiseen ovat akateemisissa piireissä suljettuja yhteiskuntamalleja houkuttelevampia. Näistä syistä erityisesti Yhdysvallat on onnistunut luomaan Piilaakson kaltaisia huippuosaamisen keskittymiä.

Tekoäly nähdään yhtenä tärkeänä osa-alueena maiden välisessä kamppailussa taloudellisesta, poliittisesta ja sotilaallisestakin vaikutusvallasta. Tekoäly tulee olemaan yhä tärkeämmässä roolissa kaikissa tietotekniikan sovelluksissa. Valtiot kilpailevat tekoälyn kehittämisen johtoasemasta ja investoivat teknologian tutkimukseen ja hyödyntämiseen. Samalla tekoälyn rooli on arkipäiväistymässä ja siitä on tullut osa jokapäiväistä elämää. Tekoälyllä ei ole enää muutaman vuoden takaista erityisasemaa muiden teknologioiden joukossa. Kyberturvallisuudessa tekoälyn käyttö on vielä kasvuvaiheessa ja sen vuoksi sen hallinta on kybermarkkinoiden toimijoille ja kyberpuolustuksen rakentajille tärkeää. ■

LÄHTEET

NIS2 JA CER – KOHTI PAREMPAA KYBERTURVAA JA RESILIENSSIÄ

https://www.nis-2-directive.com/
https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
https://www.enforcementtracker.com/
https://valtioneuvosto.fi/hanke?tunnus=SM047:00/2022

MAA-ANALYYSI: IRLANTI

https://www.ncsc.gov.ie/
https://www2.hse.ie/services/cyber-attack/
https://www.military.ie/en/who-we-are/army/army-corps/cis-corps/
https://www.gov.ie/en/consultation/a2020-national-cyber-security-strategy-2019-2024-mid-term-review-consultation/
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
https://edition.cnn.com/2022/01/23/tech/ireland-data-centers-climate-intl-cmd/index.html

TIMO RINNE

- Kyberturvallisuuden asiantuntija
- Kauppatieteen tohtori
- CISSP (Sertifioitu kansainvälinen tietoturva-asiantuntija)
- CISA (Sertifioitu tietoturvajärjestelmien tarkastaja)

OFFENSIIVINEN KYBERPUOLUSTUS

https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
https://www.hoover.org/sites/default/files/research/docs/deeks_webreadypdf_0.pdf
Jensen, M. (2022). Five good reasons for NATO's pragmatic approach to offensive cyberspace operations. Defence Studies, Vol 22 n:o 3, pp. 464-488.
https://www.nato.int/cps/en/natohq/topics_78170.htm
Goldsmith, J (ed). (2022). The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment. Oxford University Press.

KANSAINVÄLINEN KILPAILU TEKOÄLYTEKNOLOGIASTA

https://www.business-standard.com/article/technology/global-artificial-intelligence-spending-to-reach-434-bn-in-2022-report-122022000195_1.html
https://www.tortoisemedia.com/intelligence/global-ai/
https://aiindex.stanford.edu/report/
https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
https://www.researchgate.net/publication/343328470_Artificial_Intelligence_for_Cybersecurity_A_Systematic_Mapping_of_Literature

INTOHIMONA KYBERTURVALLISEMPI MAAILMA

Cyberwatch Finland

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 kehitys-kulkuja 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

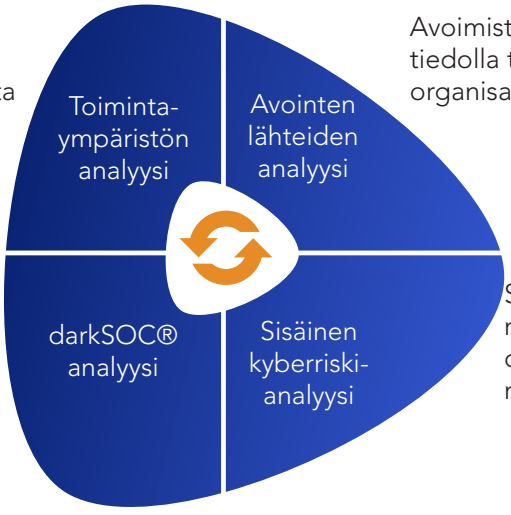
Olemme kokenut ja luotettu johdon neuvonantaja ja asiantuntija. Tuemme sinua kokonaisturvallisuuden, kyberturvallisuuden, sisäisen turvallisuuden asiakokonaisuuksissa ja kumppaniriskien hallinnassa. Työskentelymetodeinamme ovat muun muassa teema-alustukset, muistiot, työpajat ja skenaariotyöskentely.

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 kuukausi- ja kvartaalikatsauksille sekä näistä syntyville vuosiennusteille.
Viikkokatsauksen avulla saat ajantasaista kuvaa merkittävistä kybermaailman tapahtumista 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.

Kvartaalikatsaus

Kvartaalikatsaus keskittyy tarkastelujakson merkittävimpiin kybermaailman tapahtumiin.
Siinä seurataan pidemmällä aikavälillä ilmiöiden vaikutuksia ja kehityksiä.
Kvartaalikatsaus arvioi tulevaisuuskuvia sekä kehityssuuntia ja on luonteeltaan ennustava.
Kvartaalikatsauksessa on myös maa-analyysi, jossa tarkastellaan yksittäisten valtioiden kybertoimintaan liittyviä voimavaroja, uhkia ja erilaisia kyberturvallisuuden ratkaisuja.
Kvartaalikatsaus ilmestyy 4 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

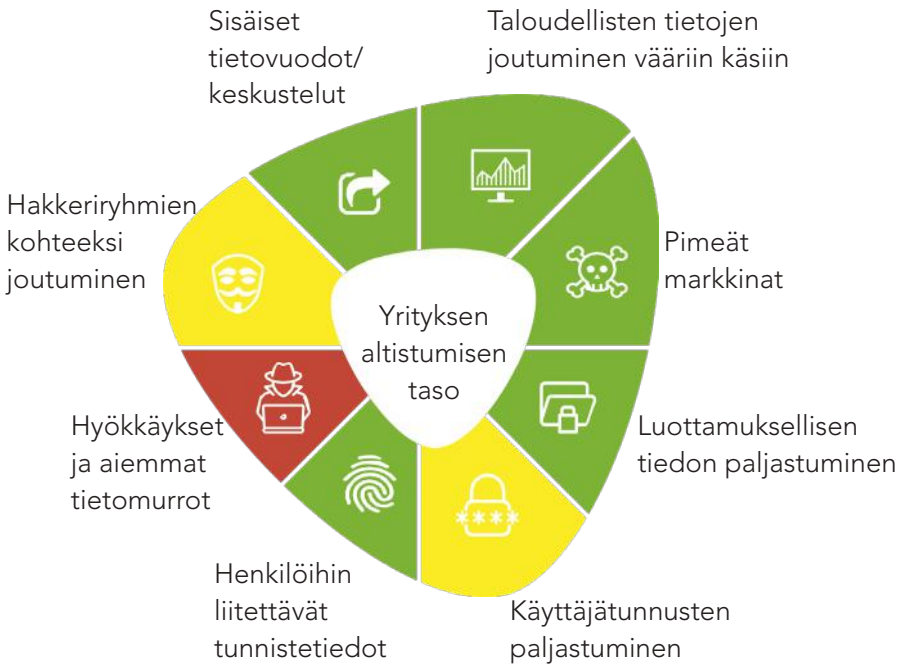
Tuotamme määrittelemästäsi teemasta, esimerkiksi tietystä toimialasta tai kohdemarkkinasta raportteja ja katsauksia: nykytilan arviointeja, uhka-arvioita, toimintaympäristöanalyyseja ja ennusteita

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 kybertiedustelukykyä
- Ennakoi kybermaailman kehityskulkuja
- Täydentää yrityksen kybermaturiteettia
- Toimii forensictutkinnan apuvälineenä
- Tukee organisaation strategista päätöksentekoa
- Täydentää strategista kybertilannekuvaa
- Löytää haavoittuvuuksia ja heikkouksia
- Fasilitoi kyberstrategiaprosessia

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

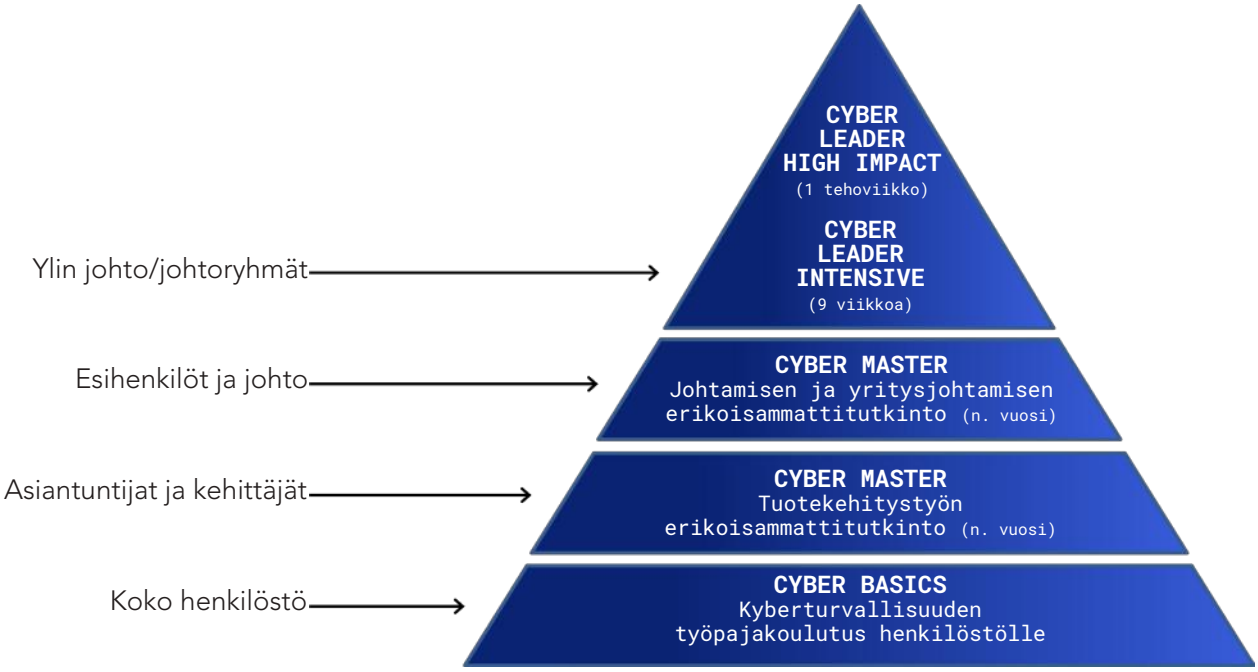
Koulutus ja osaamisen kehittäminen

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

MESSUKESKUS

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.

Read more and register at cybersecuritynordic.com

CYBER SECURITY NORDIC

7–8 November 2023
Helsinki Expo and Convention Centre

KEYNOTE SPEAKERS

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

Valentino De Sousa
Principal Director, Europe Cyber Threat Intelligence Lead
Accenture Security

Colm Murphy
Senior Cyber Security & Privacy Advisor
Global Cyber Security & Privacy Office, Huawei

Henna Virkkunen
Member of European Parliament (EPP)

INTOHIMONA KYBERTURVALLISEMPI MAAILMA

Ota yhteyttä

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
ake@cyberwatchfinland.fi