EUROOPAN SISÄINEN TURVALLISUUS MURROKSESSA

SAFERGLOBE

Miten kyberturvallisuutta luodaan rajattomassa maailmassa, Kyberalan Peter Sund?

Digitaalinen maailma on erottamaton osa reaalimaailmaa, ja kyberturvallisuus on keskeinen osa kaikkea turvallisuutta. Kyberala ry:n toimitusjohtaja Peter Sund avaa, miten rajat ylittävät kyberuhat vaikuttavat sisäiseen turvallisuuteen ja mitä voimme tehdä niiden torjumiseksi.

”Digitaalinen maailma on kiinteä osa reaalimaailmaa – ja siten sekä sisäistä että ulkoista turvallisuutta”, tiivistää Suomen kyberturvallisuusalan etujärjestö Kyberala ry:n toimitusjohtaja **Peter Sund** turvallisuuden digitaalisen ulottuvuuden.

Sundia voi luonnehtia todelliseksi turvallisuusalan ammattilaiseksi. Hänen uransa ulottuu yksityiseltä turvallisuussektorilta puolustusvoimien erikoisjoukkoihin ja edelleen lainvalvonnan tehtäviin.

Ennen Kyberalaa hän on työskennellyt myös EU:lla, ulkoasiainhallinnossa, YK:lla ja kriisinhallinnassa, jota kautta hän on saanut kattavan kokemuksen kansainvälisestä yhteistyöstä ja sisäisen turvallisuuden ulkoisesta ulottuvuudesta.

Käytännössä kyberturvallisuus tarkoittaa Sundin mukaan kyberrikollisuuden poissaoloa. Hän huomauttaa kyberrikollisuuden olevan itsessään operationaalinen termi, jonka alle sisältyy monenlaisia laissa jo muutenkin kiellettyjä tekoja, kuten tietoturvaloukkauksia ja maksuvälinepetoksia, jotka toteutetaan tietoliikenteen välityksellä.

LYHYESTI:

- Kyberturvallisuus on keskeinen osa kokonaisvaltaista turvallisuutta ja tarkoittaa kyberrikollisuuden poissaoloa.
- Kyberuhat eivät tunne valtionrajoja, joten niiden torjunta vaatii laajaa kansainvälistä yhteistyötä.
- Monet kyberrikolliset toimivat valtioista käsin, joilla ei ole kykyä tai halua puuttua alueeltaan lähteviin hyökkäyksiin, tai ne jopa hyötyvät niistä.
- Paras tapa torjua kyberuhkia on tehdä niiden toteuttaminen mahdollisimman vaikeaksi tehokkaalla tietoturvalla ja kyberturvallisuudella.
- Muita keinoja ovat mm. diplomaattiset keinot kyberrikollisuutta mahdollistavia valtioita kohtaan, tehokas rikostorjunta ja sotilaallinen puolustus.
- Kyberturvallisuutta vahvistettaessa on keskeistä määritellä rajanvedot suhteessa oikeusvaltioon, perusoikeuksiin ja yksityisyyteen.

SaferGlobe on vuonna 2010 perustettu riippumaton suomalainen ajatushautomo, joka tuottaa tietoa ja kehittää työvälineitä kestävän rauhan ja turvallisuuden edistämiseksi.

Lue lisää: saferglobe.fi

Verkkouhat eivät tunne valtiorajoja

Internet ei juuri tunne valtioiden rajoja, mikä asettaa erityisiä haasteita sisäiselle turvallisuudelle. ”Usein uhkien lähtöpisteet sijaitsevat Suomen ulkopuolella, ja ne vaikuttavat meihin suoraan tai epäsuorasti.”

Monen kyberuhan lähtöpiste on valtioissa, joissa rikollisten on helppo toimia ilman merkittävää riskiä joutua vastuuseen. ”Esimerkiksi tietyt maat eivät puutu alueeltaan lähteviin kyberturvallisuusloukkauksiin, esimerkiksi rajallisen lainvalvontakyvyn vuoksi tai koska ne eivät koe niiden kohdistuvan omaan yhteiskuntaansa.”

Usein tällaiset valtiot ovat hauraita tai romahtaneita valtioita, joiden oikeusvaltiomekanismit eivät toimi ja joiden turvallisuuskoneisto ei kykene tehokkaasti täyttämään velvollisuuttaan torjua alueellaan toimivaa rikollista toimintaa. Samat alueet voivat toimia turvasatamana myös muulle järjestäytyneelle rikollisuudelle ja terrorismille. Kyberrikollisuus monissa muodoissaan on laajalti järjestäytynyttä.

”Toisinaan nämä valtiot voivat jopa passiivisesti hyötyä petosten ja tietomurtojen vaikutuksesta talouteensa tai ainakin kansalaistensa toimeentuloon.”

Sund huomauttaa myös, että lisäksi on olemassa valtioita, jotka aktiivisesti tukevat tai itse suorittavat kyberturvallisuusloukkauksia, kuten sabotaaseja ja teollisuusvakoilua. ”Esimerkiksi Venäjä antaa toimintavapautta ryhmille, jotka edistävät maan poliittisia tavoitteita”, Sund huomauttaa.

”Äärimmillään valtioinstituutiot itse toteuttavat näitä tekoja, ja ne voivat olla erittäin hyvin resursoituja.”

Nämä niin sanotut *APT-ryhmät (Advanced Persistent Threat)* ovat järjestäytyneitä ja pitkäjänteisiä toimijoita, jotka usein yhdistävät valtiollisen tuen ja rikollisen toiminnan. Näiden ryhmien määrä on kasvanut viime aikoina tuhansilla.

”On tärkeää ymmärtää, että tekijän motiivi tai tausta ei muuta teon luonnetta rikoksena”, Sund painottaa. ”Teko on kohteessaan rikos riippumatta siitä, onko tekijä yksityishenkilö, rikollisjärjestö tai valtion viranomainen.”

Kyberrikollisuutta ei voi torjua vain kansallisin toimin

Kyberrikollisuutta on Sundin mukaan hyvin vaikea erottaa sisäisen ja turvallisuuden kysymyksiin. ”Digitaalisessa maailmassa aika ja etäisyys menettävät merkityksensä”, Sund selittää. ”Tieto ja pahat teot liikkuvat sekunnin murto-osissa maapallon toiselta puolelta.”

Tämä tarkoittaa, että perinteiset turvallisuuskäsitykset eivät enää riitä. ”Ei ole olemassa, eikä pitäisikään olla ’nettirajavartiolaitosta’, joka kontrolloisi datan laillista liikkumista valtioiden maantieteellisten rajojen yli”, Sund toteaa. ”Monet kuvittelevat, että moderni digitaalinen infrastruktuuri voi toimia kuin kansallisvaltiot keskiajalla. Kansainvälien yhteistyö on välttämätöntä.”

Torjunnan lähestymistavat Sund jakaa neljään pääkategoriaan: **tietoturvaan**, **tehokkaaseen rikostorjuntaan, diplomatian keinoihin ja sotilaalliseen kyberpuolustukseen.**

Ehdottomasti paras tapa torjua kyberuhkia on Sundin mukaan niiden tekeminen mahdollisimman vaikeaksi. Toiminta on tehtävä kannattamattomaksi ja seurauksiltaan epävarmaksi, jotta laittomaan toimintaan ei kannata ryhtyä. Tämä edellyttää tietoturvan parantamista niin yksilökuin yritystasolla sekä julkisella sektorilla, ja lisäksi teknologian kehityksessä mukana pysymistä myös tekoälyn osalta. Myös tietoturvatietoisuuden lisääminen on tässä keskeistä.

Toiseksi Sund mainitsee lainvalvonnan ja rikosprosessien merkityksen. ”On kehitettävä rikostorjuntakykyä niin, että lainvastaisten tekojen jälkeen rikosvastuu toteutuu, vaikka tekijät olisivat ulkomailla.”

Kansainvälinen yhteistyö on tässä avainasemassa. ”Samoin kuin rahanpesun ja terrorismin torjunnassa, myös kyberrikollisuuden vastaisessa työssä tarvitaan selvästi aiempaa laadukkaampaa yhteistyötä eri maiden välillä”, Sund korostaa.

Kolmantena keinona ovat diplomaattiset keinot, kuten talouspakotteet ja kansainväliset sopimukset, jotka vaikuttavat valtioihin, jotka sallivat ja tukevat kyberrikollisuutta.

Sund huomauttaa, että yksittäisen valtion mahdollisuudet toteuttaa näitä keinoja ovat ra-

jalliset. ”Esimerkiksi taloudelliset pakotteet voivat olla tehokkaita vain, jos ne toteutetaan laajassa rintamassa”, hän selittää. ”EU:n yhtenäinen linja on tässä avainasemassa.”

Ei vain kybersotaa

Neljättä keinoa, sotilaallista kyberpuolustusta, Sund varoittaa korostamasta liikaa, etenkin nykyisessä turvallisuusympäristössä.

Kybersota on täyttä todellisuutta, mutta sotatilan ulkopuolella sitä painotetaan hänen mukaansa liikaa julkisessa keskustelussa.

”Ukrainan sodan myötä on havaittu, että perinteinen sodankäynti ja digitaalinen sodankäynti kietoutuvat toisiinsa”, Sund sanoo. ”Toki on myös ns. laaja-alaista vaikuttamista aseellisen konfliktin rajan alla, mutta tämä ei ole kansainvälisen oikeuden mukaan sotaa. Kyberhyökkäykset ovat osa modernia konfliktia, ja valitettavasti ne kohdistuvat pääosin siviilikohteisiin.”

Sund kuitenkin huomauttaa, että kyberhyökkäysten luonne sotatilan ulkopuolella on säilynyt samana. ”Yhtäkään Ukrainan ulkopuolella toteutettua kyberhyökkäystä ei ole vielä tulkittu aseelliseksi hyökkäykseksi”, hän selittää. ”Hyökkääjät nimittäin ymmärtävät, että tiettyjen kansainvälisen oikeuden rajojen ylittäminen voi johtaa vakaviin seurauksiin.”

Sund ei myöskään lähtisi eskaloimaan konflikteja digitaalisilla vastaiskuilla, sillä tällöin kärsijänä ovat sivulliset. ”Sen sijaan meidän tulisi ammattitaidolla ja viekkaudella keskittyä siihen, että hyökkäyksiä ei pääse tapahtumaan.”

Sodan myötä on myös havaittu, kuinka tärkeää on kyberturvallisuuden perusasioiden hallinta. ”Monet onnistuneet kyberhyökkäykset ovat johtuneet perustason puutteista tietoturvassa”, Sund huomauttaa. ”Tämä korostaa riskienhallinnan ja tietoturvatoimien merkitystä.”

Ennaltaehkäisyä oikeusvaltion periaatteiden mukaisesti

Turvallisuuden lisääminen ei voi Sundin mukaan tapahtua oikeusvaltion periaatteiden kustannuksella. Presidentti **Niinistökin** korosti tätä hiljattain EU-raportissaan. ”On tärkeää olla tarkkana keinojen suhteen, joilla turvallisuutta väitetään parannettavan”, Sund korostaa.

Hän painottaa, että perusoikeuksia on kunnioitettava myös kyberturvallisuuden nimissä.

”Esimerkiksi vaatimukset salauksen purkamisesta rikostorjunnan nimissä voivat avata takaportteja, joita rikollisetkin voivat hyödyntää”, Sund huomauttaa. ”Vahva salaus on olennainen osa digitaalista turvallisuutta.”

Kyberturvallisuutta voi luoda myös yhteisillä tuotestandardeilla, joissa EU on erityisen vahva. ”Esimerkiksi digitaalisten tuotteiden turvallisuudessa EU voi asettaa vaatimuksia, jotka takaavat, että markkinoille tulevat laitteet ovat turvallisia. Näin itse asiassa tehdäänkin jo”, Sund selittää.

”Tämä hyödyttää alkuvaikeuksien jälkeen sekä kuluttajia että yrityksiä ja vaikeuttaa rikollisten toimintaa.”

EU:n roolia hän ei voi alleviivata liikaa. Kun tarvitsemme tehokasta rikostorjuntaa, kansainvälistä yhteistyötä, diplomatian keinoja ja ennen kaikkea tietoturvan parantamista kaikilla tasoilla, on EU Sundin mukaan voimakkaampi kuin yksikään yksittäinen jäsenvaltio.

”Se voi vaikuttaa globaaleihin pelisääntöihin ja saada aikaan todellisia muutoksia.”

Samaan aikaan korkean tason korostuessa myöskään kansalaisten omien toimien ja osaamisen merkitystä ei saa unohtaa.

”Kyberturvallisuus on myös kansalaistaito”, Sund muistuttaa. ”Mitä paremmin ihmiset ymmärtävät digitaalisen maailman riskejä ja osaavat suojautua niiltä, sitä vaikeammaksi rikollisten toiminta käy.”

SAMUEL TAMMEKANN

Artikkelisarja on toteutettu Valtioneuvoston kanslian Eurooppa-tiedotustuella hankkeelle ”Euroopan sisäinen turvallisuus Ukrainan sodan mainingeissa”.

SAFERGLOBE