

**Toimittaja Jussi Pennanen:** Erään määritelmän mukaan rikollisen toiminnan edellytys on seuraava: Motivoitunut tekijä kohtaa otollisen kohteen riittävän valvonnan ulottumattomissa. Mutta miten teknologian ja tietoverkkojen kehitys sopii tähän yhtälöön? Tekeekö tilaisuus varkaan internetaikana aiempaa useammin? Minun nimeni on Jussi Pennanen ja keskustelemme tänään kyberrikollisuudesta. Kanssani täällä Radio Moreenin ajanmukaisessa etästudiossa, on kyberrikollisuuden erityisasiantuntija Tero Toiviainen, tervetuloa

**Haastateltava Tero Toiviainen:** Kiitoksia.

**Toimittaja Jussi Pennanen:** Kyberrikollisuus on hieno termi, siitä tulee mieleen elokuvien vihreitä numeroita vilisevät hakkerointikohtaukset. Onko tämä mielikuva oikea, vai mistä oikeastaan puhumme, kun puhumme kyberrikollisuudesta?

**Haastateltava Tero Toiviainen:** Joo, oikeastaan vähän kaikki mistä kyber-määritteellä puhutaan, niin helposti vie ajatuksia tämmösiin assosiaatioihin kuin mainitsit. Kyberrikollisuudelle ei sinällään ole olemassa yhtä ainoa vakiintunutta määritelmää. Eri asiayhteyksissä sillä käytännössä tarkoitetaan toisistaan poikkeavia asioita. Mutta tämmöinen yleinen, niin meillä Suomessa kuin kansainvälisestikin tämmöinen yleinen määrittely on, että kyberrikokset on rikoksia, jotka joko kohdistuu kybertoimintaympäristöön tai tehdään kybertoimintaympäristön palveluita hyödyntäen. Eli kaksijakoinen asia.

Kybertoimintaympäristö on joko tekojen, rikosten kohteena tai sitten välineenä erilaisiin rikoksiin. Ensimmäisen ryhmän rikokset sisältää yleensä tämmösiä rikoksia joita kutsutaan ns. puhtaaksi rikoksiksi, kuten tietoverkkojen häirintä, haittaohjelmat, tämän tyyppisiä. Tämä jälkimmäinen ryhmä taas, kun kybertoimintaympäristöä käytetään tekovälineenä, pitää sisällään laidasta laitaan ihan minkälaisia rikoksia tahansa. Omaisuusrikoksia, henkeen ja terveen kohdistuvia rikoksia, mitä tahansa, mistä voi sanoa, että ovat siirtyneet tähän päivään. Kun digitaalisaatiokehitys yhteiskunnassa kehittyy, rikollisuus muuttaa muotoaan. Monet sellaiset rikokset, kuten vaikka huumausainerikokset tai petosrikollisuus, joita on ollut jo ennen internetaikaakin, niin rikosentekijät seuraavat aikaansa ja sitten siihen tulee elementtejä, joissa hyödynnetään erilaisia kybertoimintaympäristön palveluita.

**Toimittaja Jussi Pennanen:** Tästä herää kysymys, mikä sitten ei ole kyberrikollisuutta, jos kerran tämmöiset tietoverkkoja hyödyntävät rikokset lasketaan kyberrikollisuuden pariin?

**Haastateltava Tero Toiviainen:** Tää onkin hyvä kysymys. Useissa eri yhteyksissä olen nähnyt mainittavan tälläsen fraasin, kuin että kaikki rikokset ovat kyberrikoksia. En ehkä itsekään täysin allekirjoita tätä näkemystä, mutta käytännössä sen idean taustalla on juuri se, että käytännössä rikokseen kuin rikokseen voi sisältyä sellaisia elementtejä, joissa esimerkiksi niiden rikosten tutkinnassa hyödynnetään erilaisia kyberrikostorjunnan menetelmiä. Eli siitä näkökulmasta voi ajatella, että lähes kaikissa rikoksissa voi periaatteessa jonkinlaisia kybertoimintaympäristön ulottuvuuksia olla.

**Toimittaja Jussi Pennanen:** Kyllä, tämä alussa annettu kaksijakoinen määritelmä kuitenkin ehkä helpottaa tätä asian käsittelyä toistaiseksi.

**Haastateltava Tero Toiviainen:** Joo, kyllä vain.

**Toimittaja Jussi Pennanen:** Mutta jos mietitään, niin kuin toimittajat usein miettivät, tällaista Matti Meikäläisen näkökulmaa, niin millaisen kyberrikoksen kohteeksi keskiverto rivikansalainen joutuu?

**Haastateltava Tero Toiviainen:** Joo, riippuu tietysti vähän siitä, että mikä on elämänpiiri ja toimintaympäristö missä rivikansalainen toimii. Eli jos toimii tietäntyyppisissä työtehtävissä, siihen työssä voi erilaisia kyberrikoksia tulla vastaan. Mutta jos ajatellaan työstä riippumattomia rikoksia, käytännössä meillä jokaisella on, vauvasta vaariin, jonkinlaisia kytköksiä kybertoimintaympäristöön. Periaatteessa kaikki voi joutua tekemisiin kyberrikosten kanssa.

Yleisimmät rikokset on semmoiset, mitä pyritään erilaisilla massakampanjoilla saavuttamaan. Oikeastaan internetaikojen alkuvaiheesta lähtien on ollut tällaisia esimerkiksi sähköpostin massapostitukseen liittyviä asioita, ja se on edelleenkin käytössä hyvin yleisenä ilmiönä. Sähköpostin kautta tulee hyvin monenlaisia huijausyrityksiä tai monenlaisia asioita, minkä perimmäisenä motiivina on tavoitella jotakin rahanarvoista, esimerkiksi suoraa pääsyä pankkitilille tai johonkin muihin rahanarvoisiin paikkoihin. Tai sitten välillisesti saamalla jotain muuta, mitä sitten voi hyödyntää muissa rikoksissa, kuten esimerkiksi sitten mitä on ollut paljon viime vuosina: phishing-kampanjoita, eli tiedonkalastelukampanjoita. Tämmöisiä on muun muassa ilmennyt viime aikoina paljon.

**Toimittaja Jussi Pennanen:** Onko tällaista helppo havaita? Huomaako sen, että tässä on nyt kyseessä huijausyritys, vai meneekö lankaan?

**Haastateltava Tero Toiviainen:** Tässä on aika vaihteluväli. Kyllähän monet [huijaukset] on edelleen semmoisia varsin tökerösti toteutettuja ja normaali maalaisjärjellä – vai onko se nyt sitten kaupunkilaisjärki – kumpaa tahansa sovellettuna nähdään, että tässä asiassa on kyse vilpillisestä toiminnasta. Kyllähän niitä tulee edelleen paljon. Toisella laidalla on hyvinkin taidokkaasti toteutettuja tekoja. Kyllä niistä täytyy myöntää, että ei...

**Toimittaja Jussi Pennanen:** Ei voi luottaa maalais- tai kaupunkilaisjärkeen?

**Haastateltava Tero Toiviainen:** No ei, kyllä niissä tilanteissa usein on hyvin haastavia, asiantuntijoillakin saattaa olla monessa tapauksessa hyvinkin ison työn takana selvittää, että onko asiassa tosiaankin tapahtunut rikos vai ei. Mutta se täytyy sanoa, että massojen voimaan tässä aika paljon luotetaan. Yleisimmät teot pohjautuvat massaperiaatteeseen: Vaikka niissä olisi tökeröjä elementtejä, ja suurin osa ei niihin lankeaisi, ne perustuvat siihen ideaan, että jos se lähetään hyvin suurelle massalle – näitä huijauksia – niin joku saattaa tarttua siihen. Tämä on se yleinen toimintamalli. Kyllähän monet tahot, esimerkiksi poliisi, liikenne- ja viestintäministeriön Traficom ja Kyberturvallisuuskeskus usein julkaisee erilaisia tiedotteita ajankohtaisista kampanjoista, näistä varoitellaan. Niissä usein on ilmiönä se, että se kohdistuu suuriin massoihin.

**Toimittaja Jussi Pennanen:** Voiko sanoa sitten, että yleisesti ottaen on kuitenkin taso kehittynyt? Vaikka tällaisessa huijausrikollisuudessa?

**Haastateltava Tero Toiviainen:** Tää pätee oikeastaan kaikkeen rikollisuuteen...

**Toimittaja Jussi Pennanen:** Taso kehittyy jatkuvasti?

**Haastateltava Tero Toiviainen:** Jo ennen internetiä, kun jotain suojakeinoja on laadittu, niihin pyritään mukautumaan internetin puolellakin. Siinä mielessä kehittyi. Mutta kyllähän mitä meillä on Suomessa viime vuosina nähty, niissä on usein esimerkiksi käytetty suomen kieli ja sen laatu ollut viime vuosina parempaa kuin sanotaan kymmenen, kaksikymmentä vuotta sitten takaperin, kun tuli ensimmäisiä juttuja, missä jotain suomen kieltä alkoi olemaan, niin nehan saattoi usein olla hyvinkin tökeröllä suomenkielellä tehtyjä. Mut tämmösiä elementtejä sinne mukaan tulee, ja monia muitakin teknisiä elementtejä. Kyllä, totta kai ne myös seuraa aikaan, valitettavasti.

**Toimittaja Jussi Pennanen:** Rikoslaisissa ei ole kyberrikollisuudelle varsinaista määritelmää, vaan rikosnimike on usein esimerkiksi petos. Huomasin tilastoja tarkastellessani petosrikollisuudessa ison piikin yhdeksänkymmentäluvulle tultaessa. Onko teknologian kehityksellä jokin rooli tässä?

**Haastateltava Tero Toiviainen:** Nythän tosiaan ollaan siinä mistä alotettiin, eli siinä kyberrikosten määritelmässä. Jos se tosiaan näin laajasti tulkitaan se kyberrikos, että katsotaan siihen tosiaan kuuluvaksi nämä rikokset, joita kybertoimintaympäristöä välineenä käyttämällä tehdään, niin joo. Kyllähän ne ovat hyvä esimerkki sen tyyppisestä rikollisuudesta, jotka ovat niin sanotusti ajanmukaistuneet, eli siirtyneet verkkoon. Petoksiahan on tosiaan tietysti tehty jo hyvin kauan, mutta internet on tehnyt niille toisenlaisen toiminta-alustan, ja moni sellainen perinteinen petosrikos on siirtynyt verkkoihin. Se, että onko varsinaisesti rikollisuuden lisääntyminen, niin siitä on hieman erilaisiakin tutkimustuloksia.

En nyt esimerkiksi tämän petosrikollisuuden osalta ole suoranainen asiantuntija. Yleisesti on havaittu se ilmiö, että tavallaan kyberrikollisuudesta sanotaankin, että se on nopeimmin kasvava rikollisuuden laji, mutta se johtuu tietysti tästä meidän yhteiskuntamme teknologisesta kehityksestä ja digitalisaation kehityksestä. Eli kun kaikki asiat siirtyvät enemmän kybertoimintaympäristöön niin sitten rikollisuus sinällään siirtyy siinä mukana. Se on toinen asia, että lisääntyykö rikosten lukumäärä semmoisenaan. Se riippuu hieman siitä käytännön rikoksesta mistä puhutaan.

**Toimittaja Jussi Pennanen:** Eli, et ajattele niin, että teknologinen kehitys lisää rikollisuutta?

**Haastateltava Tero Toiviainen:** Tää on varmaan vähän näkökulmakysymys, siinä mielessä se lisää, että se tuo uusia keinoja ja menetelmiä. Sinällään yleisesti on tunnistettu se, että uhkapinta-ala kasvaa sitä myöten kyllä.

**Toimittaja Jussi Pennanen:** Jos mietitään tuota introssa esitettyä kysymystä, että tekeekö tilaisuus varkaan internetaikana aiempaa useammin, mitä mieltä oot tästä?

**Haastateltava Tero Toiviainen:**

Monissa rikoslajeissa se valitettavasti pitää paikkansa. Tiedyt rikosnimikkeet ennen internetaikaa oli hyvin marginaalisia siihen verrattuna mitä ne on tänä päivänä. Sieltä löytyy hyvin ikäviä

esimerkkejä muun muassa lasten hyväksikäyttöön liittyvät asiat. Siihen liittyvät rikokset ovat internetaikana lisääntyneet huomattavasti.

**Toimittaja Jussi Pennanen:** Aivan. Jos puhutaan vähän tilastoista, niin joidenkin arvioiden mukaan verkkorikoksista jää selvittämättä tilastollisesti jopa 90 prosentti. Miltä tällänen luku kuulostaa? Varmasti määritelmä [verkkorikoksen] on aika laava tässä. Tämä keskusrikospoliisin Marko Leponen joka näin on arvioinut.

**Haastateltava Tero Toiviainen:** Joo, tässä on juurikin nyt sit se, että miten missäkin asiayhteydessä on määritelty se verkkorikoksen tai kyberrikoksen määritelmä. Mutta kyllähän kaikki kansainväliset tutkimukset samansuuntaisia lukemia osoittaa. Se sitten vaan että minkä tyyppiseen prosenttiin missäkin tutkimuksessa on päädytty. Puhutaanko 90 prosentista vai 91:stä vai mistä. Mutta kyllä tutkimus selkeästi siihen viittaa.

Tämän asian todellista arviointia vaikeuttaa merkittävästi myös se, että hyvin yleisesti meillä Suomessa kuin myös maailmalla on tunnistettu sellainen ilmiö, että tämän alan rikoksia ilmoitetaan poliisille huomattavasti vähemmän, kuin mitä niitä todellisuudessa tapahtuu. Ja silloinhan ne luonnollisesti jäävät myös selvittämättä, tilastoihin päätyvä ja tulematta poliisin tietoisuuteen. Tää on hyvä kysymysmerkki, että miten tämän tyyppistä asiaa pitäisi tilastoissa käsitellä, jos siitä ei ole oikeastaan muuta kuin tällaisia etäisiä viitteitä. Mutta esimerkiksi erilaisista uhritutkimuksista mitä maailmalla on tehty, on pystytty päättämään tämä asia, että niitä rikoksia tapahtuu huomattavasti enemmän kuin mitä niitä poliisille ilmoitetaan. Niin meillä Suomessa kuin kansainvälisesti.

**Toimittaja Jussi Pennanen:** No miten tätä tilannetta voitaisiin parantaa?

**Haastateltava Tero Toiviainen:** Kyllä mä lähtisin ilman muuta tietoisuuden edistämisestä. Kyberturvallisuus on sellainen asia, jota voitaisiin pitää ihan nykypäivän kansalaistaitona. Niinku yleisetkin turvallisuusasiat: me jokainen ymmärretään, meille on tietyt asiat jokapäiväisessä käyttäytymisessä normaaleja. Kuten esimerkiksi, että lähdetään kotoa ja laitetaan ovi lukkoon. Ja kun liikenteessä liikutaan niin jatkuvastihan me tehdään tietäntyyppistä käyttäytymisen arviointi turvallisuuden suhteen. Samantyyppisiä elementtejä meidän pitäis tuoda sitten kyberturvallisuusympäristössä liikkuessamme mukaan.

**Toimittaja Jussi Pennanen:** Sen sijaan, että muutetaan tieliikennelakia, laitetaan autoihin turvavyöt? Tällaista lähestymistapaa?

**Haastateltava Tero Toiviainen:** No nyt kun otit tuon turvavyöanalogian, esimerkin, siinähan on nyt sitten kyse tämmöisestä yksittäisestä, sanotaan teknisestä suojaimekanismista. Ne on osa tätä kyberturvallisuuden rakentamista, mutta pitää muistaa, että aina kaikista tärkein on kuitenkin se itse toimija eli se ihminen itse. Meidän kaikkien käyttäytyminen ja tietoisuus asiasta. Eli ihmisten tietoisuuden lisääminen on se kaikkein tärkein asia. Totta kai me vaaditaan erilaisia teknisiä mekanismeja ja menetelmiä esimerkiksi laitteiden ja ohjelmistojen kehittäjiltä, mutta ihan tämmöistä yleistä tietoisuutta.

Se lähtee, niin kuin sanoin tuossa: vauvasta vaariin tää asia meitä koskettaa. Se pitää pienestä pitäen lähteä, aluksi vanhempien ja koulun, sitten työelämässä tuoda asiaan liittyvää tietoisuutta. Näitähan on erilaisia hyviä, muun muassa viranomaisten laatimia kampanjoita. Tässä voisin muun muassa mainita Poliisiammattikorkeakoulun ja Jyväskylän ammattikorkeakoulun tämmöisen yhteisen Cyberdi-projektin ja sen puitteissa toteutettavan Ole tietoinen-kampanjan. Sen löytää esimerkiksi ihan Google hakukoneeseen laittamalla hakusanat: Ole tietoinen. Todennäköisesti ihan ensimmäinen ja ensimmäiset linkit vievät Jyväskylän ammattikorkeakoulu JAMK:n sivuille tänne Cyberdi-projektin Ole tietoinen-kampanjaan. Sieltä löytyy paljon yleisiä asioita. Se on käynnissä oleva kampanja ja kehittyy, ja sinne tulee jatkuvasti uutta tietoa. Semmoset on hyviä muun muassa. Ja tuossa tulikin aiemmin mainittua Keskusrikospoliisin Kybertorjuntakeskus ja Traficomin Kyberturvallisuuskeskus. Näiden molempien sivuilta löytyy oikein mainioita ohjeita ja ajantasaista tietoa. Ajantasaiseen tietoon liittyen, tämän kyberturvallisuuskeskuksen erinomainen Kybersää on tämmönen mikä kuukausittain laaditaan. Eli jos hakukoneeseen laittaa Kybersää, niin varmaankin päätyy suoraan tänne Kyberturvallisuuskeskuksen sivuille. Siellä on erinomaista, hyvin yksinkertaisessa muodossa esitettyä tietoa erilaisiin kyberturvallisuusasioihin liittyen.

**Toimittaja Jussi Pennanen:** Kyllä, siinä oli loistava tietoisku sitten, miten lähteä tilannetta muuttamaan. Olemme tänään keskustelleet kyberrikollisuudesta ja vähän siitäkin miten rikollinen toiminta muuttuu teknologisen kehityksen mukana. Tero Toiviainen, kiitos haastattelusta.

**Haastateltava Tero Toiviainen:** Paljon kiitoksia.