02 Kyber
Äänitteen kesto: 32 min

Litterointimerkinnät

Haastattelija:	Harri Vänskä
Vastaaja:	Maria Keinonen

sa-	sana jää kesken
(sana)	epävarmasti kuultu jakso puheessa tai epävarmasti tunnistettu puhuja
(-)	sana, josta ei ole saatu selvää
(--)	useampia sanoja, joista ei ole saatu selvää
, . ? :	kieliopin mukainen välimerkki tai alle 10 sekunnin tauko puheessa

---

[Musiikkia]

INTRO: Kuuntelet Maanpuolustuskorkeakoulun Sotataidon ytimessä-podcastia. Jaksoissa sotataidon asiantuntijat keskustelevat ajankohtaisista yhteiskuntaan ja sen turvallisuuteen liittyvistä kysymyksistä.

HARRI VÄNSKÄ: Hei! Tervetuloa mukaan, Sotataidon ytimeen olemme matkalla. Nyt nostamme katseet Suomen kyberturvallisuuden tulevaisuuteen ja pohdimme mitä se tuo tullessaan. Minun nimeni on Harri Vänskä ja asiantuntijamme on majuri Maria Keinonen Maanpuolustuskorkeakoulusta, tutkija ja väitöskirjaansa valmisteleva tohtoriopiskelija. Kertoisitko meille nyt alkuun miten löysit kyberin vai sekö on löytänyt sinut?

MARIA KEINONEN: Ensinnäkin kiva olla mukana keskustelemassa kyberistä. Se on mun sydäntä lähellä. Mä sanoisin, että kyber ehkä löysi minut. Olin jo ennen kuin kyber-sanaa käytettiin tiedostava mitä tulee tietojärjestelmien käyttöön, sosiaaliseen mediaan. Sitten kun kyberistä alettiin puhua enemmän, niin se tuntui tämmöselle viestimiehelle oikein sopivalta ja kiinnostavalta alalta. Sittenpä mä 2016 lähdin sitä ihan opiskelemaan Jyväskylän yliopistoon.

HARRI VÄNSKÄ: Liittyykö kyber sinun väitöskirjatutkimukseen?

MARIA KEINONEN: Liittyy kiinteästi. Mun väitöskirjatutkimuksen aiheena on pienen valtion kyberpelote. Pelotehan tarkoittaa tämmöstä miten valtio viestii omista suorituskyvyistään ja koettaa ikään kuin pelottelemalla ennaltaehkäistä sitä, että toinen valtio ei tekis mitään uhkatoimia tai ei-sallittuja asioita sille puolustavalle valtiolle. Mun väitöskirjatutkimuksessa mä pohdin sitä miten kyberpelotetta vois tämmösessä yhteydessä toteuttaa.

HARRI VÄNSKÄ: Erittäin mielenkiintoista ja varmaan kuulemme siitä myöhemmin vielä lisää. Kertoisitko tähän vielä alkuun semmosen kylmäävän esimerkin kyber-keissistä, joka nousee mieleen?

MARIA KEINONEN: Mä pohdin tätä, että mikä ois hyvä esimerkki. Kaikkihan tuntee Stuxnetin, niin sitä mä en ottanut tähän esimerkiksi. Mä otin semmosen esimerkin, mikä on mua itteeni kiinnostanu ja tää ei oo mikään yksittäinen tapahtuma, vaan ehkä enemmänkin valtion tapa toimia. Esimerkki on Ukraina ja Venäjän toiminta Ukrainassa. Nyt jälkeenpäin on ehkä helpompikin tunnistaa niitä asioita mitä kybervaikuttamiseen liittyen siellä on puolin ja toisin konfliktin osana tehty. Mä nostan sotilaallisen esimerkin ja ehkä ei-niin-sotilaallisen, että miten kybervaikuttamista joku valtio voi tehdä.

Sotilaallinen esimerkki. Siellä Ukrainassa Venäjä nerokkaasti hyväksikäytti esimerkiksi GSM-puhelimia, paikansi niitä ja niiden paikannusten perusteella saattoi johtaa tykistötulta Ukrainan joukkoihin. Taikka jopa lähettää Ukrainan sotilaiden kännyköihin propagandaviestejä tai valheellista tietoa sisältäviä viestejä. Mun mielestä tää oli nerokas esimerkki siitä miten jokapäiväiset arjen välineet voi kääntyä meitä vastaan.

Toinen esimerkki oli vuonna 2015, kun Venäjä joulukuussa vähän kylmempään aikaan toteutti kyberiskun Ukrainan sähkövoimalaan. Siinä sitten sähkö katos noin 200 000 ukrainalaiselta. Tää oli mun mielestä hyvä esimerkki siitä miten joku valtio voi kohdistaa toimintaa yhteiskunnan kriittiseen infrastruktuuriin.

HARRI VÄNSKÄ: Monesti nämä termit, kyberturvallisuus ja hybridi, hybridivaikuttaminen, hybridioperaatiot, ne pyörii tämmösessä sanojen neliössä, kuusiossa tai montako niitä mukaan sit lasketaan. Miten sinä näet tämän sanakehikon?

MARIA KEINONEN: Sotilas ehkä ajattelee, että hybridi- tai laaja-alainen vaikuttaminen on joukkokeinoja, joista osaa keinoja voidaan toteuttaa ikään kuin jo normaali oloissa tai sodan kynnyksen alapuolella. Mä sanoisin, että kybervaikuttaminen ja kaikki mikä kohdistuu nimenomaan kybertoimintaympäristöön on tämmöstä. Eli kyber kuuluu siihen laajan keinovalikoimaan, kun puhutaan hybridisodankäynnistä tai laaja-alaisesta vaikuttamisesta.

HARRI VÄNSKÄ: Eli se on aina mukana, vaikkei mitään päälle näkisikään?

MARIA KEINONEN: Mä en voi väittää, että kyber olis aina mukana, mutta se on sen verran herkullinen keino siinä keinovalikoimapakissa, että se hyvin suurella todennäköisyydellä on mukana. Kybervaikuttamiseen voidaan yhdistää siis esimerkiksi informaatiovaikuttamista myös.

HARRI VÄNSKÄ: Olisiko sinulla semmosta napakkaa määritelmää kyberille ja sen vieressä oleville sanoille?

MARIA KEINONEN: No kyber sanana on vain etuliite. Se yleensä liitetään johonkin toiseen sanaan ja sillä tavalla halutaan korostaa termin kyber sidonnaisuutta. Jos me katotaan virallisia määritelmiä, niin kybertoimintaympäristö koostuu digitaalisesta ympäristöstä laitteineen ja siitä informaatiosta mitä niillä laitteilla siinä ympäristössä käsitetään.

Mut mä sanoisin, että sotilas käsittää ton vielä vähän laajemmin. Eli puhutaan, että on looginen kerros, fyysinen kerros ja käyttäjäkerros. Eli tunnustetaan ja tunnistetaan, että kybertoimintaympäristö ei oo pelkkää nollaa, ykköstä ja bitiä, vaan siihen aina liittyy ne käyttäjät. Sitten siihen aina liittyy ne fyysiset laitteet ja fyysiset tiedonsiirtovälineet, esimerkiks valokuitu tai joku tämmönen.

HARRI VÄNSKÄ: Hyvin monet yhteiskuntien kriittiset toiminnot, kuten pankit, rahoituskaupat, energiatuotanto ja muu, nämä on kaikki riippuvaisia tietojärjestelmistä ja verkkojen toimivuudesta. Eli puhutaan yhteiskuntien toimivuuden ytimestä, eikö vaan?

MARIA KEINONEN: Joo, kyllä näin. Kun tarkastellaan länsimaisia valtioita ja varsinkin Suomea, niin Suomihan on äärimmäisen riippuvainen informaatioteknologiasta. Otetaan mikä tahansa palanen pois, vaikka pankkipalveluiden toimivuus, raha ei liiku ja ihmiset ryntää nostamaan käteistä, käteinen on pian loppu. Sehän vaikuttaa kaikkeen, ihan yksilön arkeen. Voitko käydä kaupassa, voitko ostaa lääkkeitä, miten tavarat liikkuu, voiko kuljetusyhtiöt toimia, matkustamiseen ja niin edelleen. Eli kaikki suomalaisen yhteiskunnan kriittiset toiminnot on jollain tavalla riippuvaisia tai kytköksissä kybertoimintaympäristöön.

HARRI VÄNSKÄ: Ja se kaikkein suurin kysymys on: ovatko nämä turvassa?

MARIA KEINONEN: Niin. Se on hyvä kysymys, johon en ehkä uskallakaan vastata. Sanoisin, että niitä pyritään turvaamaan ja suojaamaan. Mutta samaan aikaan, vähän niin kuin ropisee peltikattoon, niin siellä on aina joku yrittämässä sisään johonkin tiettyyn järjestelmään. Vois väittää, että kyberhyökkäys pääsee aina lopulta läpi. Mä sanoisin, että tässä ei oo tärkeetä se kyetäänkö rakentaa niin vankka suojamuuri että mikään ei tuu läpi, vaan tärkeetä on toipumiskyky. Se että meillä on joku varamenetelmä, varasovellus tai varapalvelu tai se että meillä on ohjeistus miten toimitaan, kun se sade sieltä ropisee sisään. Ennen kaikkea kyky palautua siitä hyökkäyksestä, että miten palautetaan järjestelmät ja myös ihmisten luottamus niiden järjestelmien toimintaan.

HARRI VÄNSKÄ: Minkä tahon tai kenen vastuulla tämä Suomessa on, että tää toimii, palautuminen on mahdollista ja ehkäisyn kyky on suuri?

MARIA KEINONEN: Tässä tullaan yhteiskunnan kokonaisturvallisuuteen ja myös kyberturvallisuuteen. Eli kyberturvallisuus sanana voidaan käsittää koskemaan koko suomalaista yhteiskuntaa ja etenkin yhteiskuntaa pyörittäviä kriittisiä järjestelmiä ja palveluita. Se ei oo minkään yksittäisen tahon vastuulla, vaan kyber-Suomea puolustaa viranomaiset, sitä puolustaa myös organisaatiot jotka suojaa itse oman toimintansa. Ennen kaikkea kyber-Suomea puolustaa ja suojaa yksilöt eli tässä korostuu myös yksilön osaaminen, tieto ja vastuu.

HARRI VÄNSKÄ: Mikä on sotaväen rooli tässä kokonaisuudessa?

MARIA KEINONEN: Puhutaan kyberpuolustuksesta eli jo tossa selonteossa ja kyberturvallisuusstrategiassa määritellään puolustusvoimille vastuu toteuttaa kyberpuolustusta. Toi tarkoittaa niitä sotilaallisia keinoja millä turvataan vähintään puolustusvoimien omat järjestelmät, mutta myös osallistutaan kyberturvallisuuden rakentamiseen.

HARRI VÄNSKÄ: Eli sotaväki turvaa omat järjestelmänsä ja antaa tukea sitten sille, että valtiolliset muut systeemit toimii?

MARIA KEINONEN: Joo. Puolustusvoimien tehtävissä määritetään, että puolustusvoimien pitää turvata Suomen alueellinen koskemattomuus ja siellä on myös velvoite antaa virka-apua. Eli jos joku toinen viranomainen puolustusvoimia lähestyy virka-apupyynnöllä, niin sitten puolustusvoimat myös tässä kybertoimintaympäristössä voi auttaa.

HARRI VÄNSKÄ: Voidaanko ajatella, että kun kyberpuolustus on päällä, niin siihen kuuluu myöskin kyky tehdä kyberhyökkäyksiä?

MARIA KEINONEN: Joo, kyllä näin voidaan ajatella. Varsinkin kun tää on ihan julkisesti selontekoon kirjattu, että puolustusvoimilla tulee olla kyky myös vaikuttaa, siis kybervaikuttaa ja myös kybervastatoimiin. Vastatoimilla tarkoitetaan, että jos joku hyökkää, niin miten siihen sitten reagoidaan. Eli ei pelkästään puolusteta, vaan voidaan myös iskeä takaisin.

HARRI VÄNSKÄ: Tästä ilmeisesti kovin vähän annetaan tietoa julki?

MARIA KEINONEN: No näin on. Siis tää on ihan yleinen trendi, mitä tulee kybertoimintaympäristöön ja oikeastaan kaikkien maailman valtioiden toimintaan. Valtiot haluaa salata sen todellisen kybersuorituskykynsä eli ei haluta kertoa millaisia todellisia vaikutuksia jollain hyökkäyksellä on ollut tai ei haluta kertoa miten niihin on reagoitu. Tää on ihan tunnistettu trendi miten eri valtiot toimii tässä kyberasiassa.

HARRI VÄNSKÄ: Strategia on eräs lempi sanoista, mitä puolustusvoimissa käytetään. Onko olemassa myöskin erillinen kyberstrategia?

MARIA KEINONEN: Kyberturvallisuusstrategia on kirjoitettu itse asiassa kahteen kertaan, vuonna 2013 ja -19. Tää koskee yhteiskunnan kyberturvallisuutta. Semmosta erillistä kyberpuolustusstrategiaa ei oo kirjoitettu, missä strategiatason asiakirjoissa sitten määriteltäis nimenomaan niitä puolustusvoimien velvollisuuksiin kuuluvia asioita. Mut nää yhteiskunnan kyberturvallisuusstrategiat on tosiaan tässä viime vuosikymmenellä kahteen kertaan kirjoitettu ja julkaistu.

HARRI VÄNSKÄ: Tämä liittyy varmaan ihan olennaisesti siihen millä tavalla tulevaisuuden sodankäynti kehittyy? Majuri Maria Keinonen, mikä on sinun arviosi siitä mikä on kehityksen trendi?

MARIA KEINONEN: Tää onkin mielenkiintoinen juttu. Se on ehkä vähän kuollut termi, että teknologian kiihtyvä kehitys, mutta kun se on totta ja mä joudun nyt käyttää sitä samaa termiä tässä. Eli onhan se niin, että teknologia myös tekee tiensä asevoimiin ja taistelukentille. Nyt ehkä semmosia teknologiaan liittyviä trendejä on tekoäly. Esimerkiksi Venäjä on Syyriassa testannut tämmösiä itsestään liikkuvia miinanraivausrobotteja, jotka kykenee tekee päätöksiä. Ei välttämättä hirveän hyvällä menestyksellä, mutta on nähtävissä, että tähän suuntaan halutaan mennä. Halutaan ehkä ihminen pois sieltä pahimmasta tulesta ja taistelusta ja laitetaan sinne se robotti, joka osaa ehkä ajatella itse tai tehdä jonkin tason päätöksiä itse. Eli toi on ainakin yksi trendi.

Toinen trendi. Palataan taas siihen laaja-alaiseen vaikuttamiseen ja miten toimitaan sodankäynnin kynnyksen alapuolella. Ei oo enää helppo tehdä eroa sille milloin ollaan taisteluissa, sodassa tai mikä on se tietty ajan hetki. Ei välttämättä enää laukaista Mainilan laukauksia tai marssita fyysisesti jonkun toisen valtion rajan yli. Se saattaa tapahtua kybertoimintaympäristössä ja siihen saattaa liittyä informaatiovaikuttamista. Siihen saattaa liittyä erilaisia hybridivaikuttamisen keinoja, kuten lietsotaan maan sisäistä levottomuutta tai laitetaan pakolaisia tulvimaan rajan yli. Se voi olla kaikkee tällaista.

HARRI VÄNSKÄ: Tarkoitatko sitä, että hyvinkin rajuja kybertaisteluja voidaan käydä julkisuudelta piilossa?

MARIA KEINONEN: Joo. Ja mä väitän, että niitä käydään joka päivä.

HARRI VÄNSKÄ: Suomessakin?

MARIA KEINONEN: Kyllä. Välttämättä kyse ei ole taisteluista sotilaallisessa mielessä. Ehkä suurin osa arkipäivän tapahtumia liittyy rikolliseen ja sitä kautta rahan hankintaan tai tiedon hankintaan, voidaan puhua teollisuusvakoilusta tai valtiollisesta tiedonhankinnasta. Mutta kyllä mä väitän, että sen rinnalla käydään myös ihan aitoja kybertaisteluita, missä jokin valtio kybertaistelee toista valtiota vastaan. Se ei vaan nouse pinnalle, niin kuin mä aikaisemmin totesin, että valtiot ei halua paljastaa omia suorituskykyjään, niin niistä ei sitten tiedoteta.

HARRI VÄNSKÄ: Viime vuonna Suojelupoliisi tunnisti eduskuntaan kohdistuneen valtiollisen kybervakoiluoperaation, siis suomalaisen kansanvallan ytimeen, jossa yritettiin tunkeutua eduskunnan tietojärjestelmiin. Onks tämä tähän mennessä nähdyistä ehkä merkittävin?

MARIA KEINONEN: Niin, täs vois miettiä, että merkittävin miltä kannalta? Siltä kannalta, että sitä yritettiin tai että se onnistui tai että sillä oli jotain vaikutusta. Mä en ehkä osaa tohon merkittävyyteen vastata. Mutta mun mielestä on hyvä osoitus, kun näitä ajoittain nousee pinnalle, että siellä koko ajan tapahtuu jotain. Tämmöseskin tapauksessa voi olla kyse siitä, että jossain järjestelmässä ollaan oltu sisällä jo vuosikausia ja sitten joko on jääty kiinni tai sitten on jokin ajan hetki, että se tunkeutuja on päättänyt, että nyt pistetään sivut kyykkyyn tai jotain muuta vastaavaa.

HARRI VÄNSKÄ: Ulkoministeriössähän oli tällainen tapaus, jossa aika pitkän, vuosien toiminnan jälkeen vasta kävi ilmi, että sieltä oli kadonnut tietoa.

MARIA KEINONEN: Joo, kyllä näin on. Näitä kutsutaan advanced persistent threat eli semmonen pitkäaikainen uhkatoimija, joka ujuttautuu järjestelmään ja sitten se siellä tyytyväisenä kenenkään huomaamatta ehkä varastaa tietoa tai valmistelee jotain muuta kampanjaa. Jossain vaiheessa se joko huomataan, poistetaan tai sitten se uhka pääsee laukeamaan.

HARRI VÄNSKÄ: Ovatko nämä tiedon ronkkijat valtiollisia vai kaupallisia toimijoita, jotain siltä väliltä vai rikollisia?

MARIA KEINONEN: Voisin sanoa, että varmaan kaikkia näitä tietyssä määrin. Mä uskoisin, että valtiollisia toimijoita kiinnostaa semmoset kohteet millä on jotain strategista merkitystä tai merkitystä sen yhteiskunnan toiminnalle. Taikka sitten se kohde on semmonen, josta saadaan kiinnostavaa tiedot. Rikolliset luultavasti haluaa ennen kaikkee hyötyä rahallisesti eli se kohde voi olla esimerkiksi pankkijärjestelmä tai nyt kun bitcoinit on suuressa huudossa, niin siihen liittyviä huijauksiakin on esiintynyt aika paljon. Mut en mä suljis pois teollisuusvakoilua, niin kuin aikaisemmin mainitsin. Myös tämmöset yksilöt, jotka joko haluaa testata, se on kivaa ja kaverin kanssa ollaan lyöty vetoa, tai sitten on joku idealismi taustalla. Ehkä viimeisenä ryhmänä terroristit.

HARRI VÄNSKÄ: Niin, mehän on nähty Suomessakin, että teini-ikäiset pojat ovat saaneet suuren verkkopankin pois raiteiltaan.

MARIA KEINONEN: Niin, tässä lienee kyse semmosesta uteliaisuudesta, joka on ehkä konkretisoitunut vähän väärällä tavalla. Itse asiassa poliisilla on tämmönen, en nyt muista nimeä, se oli jonkinnäköinen kyber exit-ohjelma, jossa kybersuuntautuneita

nuoria koetaan kaitsea pois rikollisuudesta ja enemmän hyvää tekevän hakkeroinnin puoleen.

HARRI VÄNSKÄ: Muistan lukeneeni tai kuulleeni sellaisenkin arvion, en tiedä varmasti pitääkö se paikkansa, mutta kaikkein salaisin tieto erään lähteen mukaan, jota raportoidaan vaikka valtion johdolle ulkomailta, kirjoitetaan joku raportti, se kirjoitetaan perinteisellä vanhanaikaisella kirjoituskoneella ja laitetaan kuriiripostilla matkaan, koska tietojärjestelmiin ei voi täysin luottaa. Onks tää uskottavaa?

MARIA KEINONEN: Kyllä mä voisin tän hyvin uskoa siinä mielessä, että oli sitten internetiin kytketty tai ihan täysin internetin ulkopuolinen järjestelmä, niin jos siinä on laitteita jotka käsittelee digitaalisesti tietoa, niin jos siihen ympäristöön ei pysty ikään kuin verkon kautta tunkeutumaan, niin siihen ainakin pystyy tunkeutumaan niin, että meet paikan päälle ja pyydät työntekijältä salasanan ja sitten meet käyttää tietokonetta. Eli mikä tahansa digitaalinen väline, oli se sitten kännykkä, älykello, tietokone tai ympäristö suljettu tai avoin, niin tavalla tai toisella se on korkattavissa.

HARRI VÄNSKÄ: Ja kaikkein kriittisin pointti, taho, tekijä on edelleenkin ihminen?

MARIA KEINONEN: Juuri näin. Yksilö on kyberturvallisuuden heikoin lenkki. Näin mä väitän, koska ihmisistä koostuu organisaatiot, yhteisöt ja se turvallisuuskokonaisuus. Eli esimerkiksi jos jossain organisaatiossa yks ihminen klikkaa auki väärän sähköpostiviestin, niin siinä voi pahimmassa tapauksessa levitä joku mato koko sen organisaation järjestelmiin. Mun mielestä ehkä helpoin muistettava ja tärkein kyberturvallisuusohje on kaikille meille: älä klikkaa.

HARRI VÄNSKÄ: Niin siis, älä tee mitään?

MARIA KEINONEN: Ton takana on sanoma, että jos sulle lähetetään yllättävästi jotain, kaveri lähettää jonkun linkin ja siinä ei oo mitään saatesanoja tai se kaverin käyttämä kieli tuntuu omituiselta, tai jos Facebookin sivuilla kaveri jakaa jotain mielenkiintoista, jotain tarjouksia tai mitä vaan, tai jos tulee sähköposti tai tekstiviesti, mistä et voi olla ihan varma, niin älä klikkaa. On semmosia teknisiä keinoja miten voi tarkistaa esimerkiksi jonkun sähköpostiosoitteen oikeellisuuden, mutta-

HARRI VÄNSKÄ: Väsyneenä ja kiireessä ja-

MARIA KEINONEN: Niin, kyllä. Mun täytyy myöntää, että mäkin oon joskus saanut ihan jonkun sosiaalisen median viestintäsovelluksen kautta kaverilta videon. Olin jo menossa klikkaamaan, koska se on luonnollista että lähetellään hassuja kuvia. Mut sit joku epäilys heräs ja sormi pysähtyi. Sit mä kävinkin kyberturvallisuuskeskuksen sivuilla kattomassa, että siinä tietyssä sosiaalisen median viestintäsovelluksessa leviää virus, joka on kohdistettu nimenomaan Apple-puhelimille. Eli jos käyttäjä sitä käy klikkaamassa, niin se antaa viruk-

HARRI VÄNSKÄ: Sinne menee.

MARIA KEINONEN: Niin, antaa luvan sille virukselle levitä.

HARRI VÄNSKÄ: Miten sinä huolehdit tästä kyberhygieniasta?

MARIA KEINONEN: Ensinnäkin mä en klikkaa. Sit toisekseen mä oon huolehtinut, että kaikissa mun älylaitteissa, eli kännykkä, tabletti, tietokonen yms. yms., kaikki tämmöset älykkäät laitteet, mulla on ajantasainen viruksentoimintaohjelmisto. Jonkun tutkimuksen mukaan yllättävän moni ihmisistä unohtaa hankkia semmosen kännykkään. Mun mielestä se on aika hälyttävää. Eli joka laittees pitää olla oma turva. IoT-laitteet on ongelma, koska tällaisia ominaisuuksia ei välttämättä sisäänrakennettu niihin. Eli joku vanhanmallinen imuri voi vahingossa sinusta kerätä tietoa kodistasi haluamattasi. Anyway. Toinen on semmonen terve harkinta ja malli. Ja mä toistan taas, että älä klikkaa. Se on mun mielestä kaikkein tärkein.

HARRI VÄNSKÄ: Palataan vielä kansainväliseen yhteistyöhön, joka on kyberteemassa varmaan kaiken A ja O. Pärjääkö Suomi yksin vai onko sen pakko liittoutua, antaa tietoa ja ottaa tietoa muualta, olla tiiviissä vuorovaikutuksessa muitten kanssa?

MARIA KEINONEN: Mä väitän, että yksin ei pärjää kukaan. Suomessa viranomaiset ei voi toimia pelkissä omissa siiloissaan yksin ja myös Suomi valtiona tarvii tukeaa. Se ei tarkoita, että kaikki tehtäis yhdessä. Suomihan on mukana esimerkiksi Euroopan unionin kyberturvallisuuden kehittämisessä ja on sitoutunut EU:n kyberturvallisuusstrategian määrittämiin asioihin. Ja Suomessa viranomaiset tekee yhteistyötä. Mut tällä hetkellä musta tuntuu, että se ei ehkä riitä. Kybertoimintaympäristö on globaali ja internetissä ei oo valtion rajoja, niin tää tekee ehkä kyber-Suomen puolustamisesta niin monimutkaisen tapauksen, että jonkn verran yhteistyötä on välttämätöntä tehdä muiden valtioidenkin kanssa.

HARRI VÄNSKÄ: Eli nimenomaan niitten kanssa, joilla on joku korkea teknologiaosaaminen ja huippu tieto ja taito?

MARIA KEINONEN: Niin, se voi olla. Se yhteistyö kohdituu osaamiseen vaihtamiseen tai tiedon vaihtamiseen tai tutkimusyhteistyöhön tai mihin vaan oikeastaan. Mä uskon, että kaikissa näissä osa-alueissa Suomi voi sekä hyötyä että olla hyödyttämässä muita kyberyhteistyössä.

HARRI VÄNSKÄ: Kyberturvallisuus on varmaan myöskin liike-elämässä eräs tulevaisuuden suuri kilpailuetu. Voisiko Suomi yrittää rakentaa itsestään eräänlaista fortress Finlandia, linnaketta jossa ois täällä toimiville yrityksille, yhteisöille ja organisaatioille tarjolla tavallista parempaa suojaa?

MARIA KEINONEN: Tää linnake-termi nostaa heti semmosia mielikuvia-

HARRI VÄNSKÄ: Aitoja.

MARIA KEINONEN: Aidoista, tai linnoista mitä oli ennen vanhaan. Nythän moni kuulija varmaan tietää, että Venäjällä on tavoitteena muodostaa tämmönen kyberlinnake. Eli keinot, joilla Venäjä pystytään irrottamaan globaalista internetistä. Mä sanoisin, että Suomen ei kannata tämmöstä lähteä puuhaamaan ja se ei oikein meidän kansalliseen identiteettiinkään sovi tai Suomen tapaan hoitaa asioita. Mut ehkä Suomi pystyy just tällä kyberyhteistyöllä ensinnäkin herättämään luottamusta. Luottamus voi olla ikään kuin se kyberlinnake, mikä ehkä vois sitten houkutella muita toimijoita Suomeen. Se luottamus voi rakentua yhteistyön lisäks suomalaisen yhteiskunnan tavasta reagoida ja vastata kyberuhkiin ja erityisesti siitä miten me osoitetaan omaa resilienssiä eli toipumiskykyä.

HARRI VÄNSKÄ: Suomalaiset yleensä aina mielellään vertailevat itseään naapureihin erityisesti Ruotsiin. Ollaanks me Ruotsin kanssa samalla viivalla vai kumpi on tässä parempi?

MARIA KEINONEN: Ylipäätään eri valtioiden vertaileminen keskenään on aika haastavaa, koska saattaa olla pikkasen eri lähtökohdat tehdä kyberturvallisuutta tai yhteiskunnan kokonaisturvallisuutta yleensä. En tässäkään nyt halua laittaa meitä mihinkään järjestykseen, et tuliko Suomi vai Ruotsi ensin, mut mä sanoisin, että meillä on hyvä yhteistyö jo menossa ja myös paikkoja kehittää sitä kyberyhteistyötä. Mä luulen, että monessa mielessä Suomi ja Ruotsi on jo arvoiltaan ja henkisestikin aika lähellä toisiaan ja valmius tehdä sitä yhteistyötä on hyvä.

HARRI VÄNSKÄ: Palataan tässä lopuksi vielä sinun väitöskirjaasti, majuri Maria Keinonen. Koska se valmistuu?

MARIA KEINONEN: No niin, tää on aina tohtoritutkijalle kuumottava kysymys, varsinkin kun on juuri aloittanut työnsä. Uskallan väittää, että seuraavien vuosien aikana, ei vuosikymmenten, vaan vuosien. Jos saa mainostaa, mulla on kolme tieteellistä artikkelia ens vuonna lähdössä arviointikierrokselle ja aiheiltaan ne tulee koskettamaan pienen valtion kykyä muodostaa pelote tai pidäke, kyberyhteistyötä, mistä mä oon tosi kiinnostunut ja sitten näistä vielä ehkä se kolmas artikkeli on jalostettu eteenpäin ajatuksina. Mutta jos joku kiinnostui tästä, niin mielellään sitten myös jaan tietoa. Näähän on ihan julkisia, tohtoriväitöskirjaan tai kirjoitukseen liittyvät julkaisut.

HARRI VÄNSKÄ: Hyvä. Kiitoksia sinulle ja onnea matkaan.

MARIA KEINONEN: Kiitoksia. Oli mukavaa käydä täällä.

[Musiikkia]