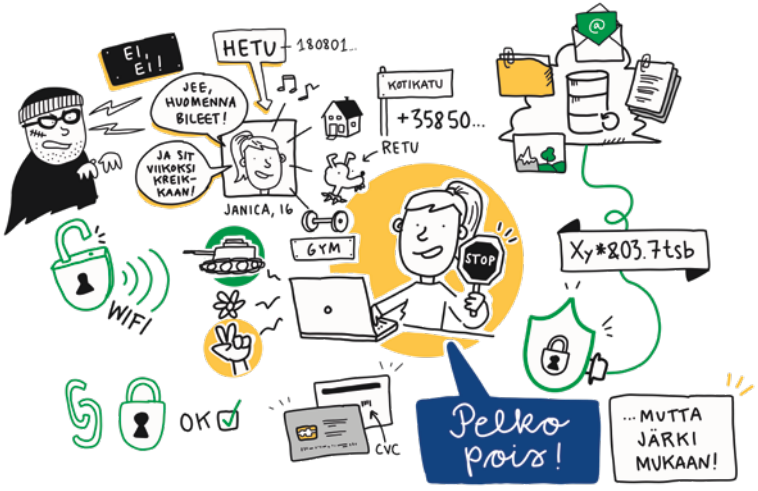
KYBERIN TASKUTIETO

KESKEISIN KYBERMAAILMASTA JOKAISELLE

Irina Lönnqvist ja Panu Moilanen



MIKSI SINÄ TARVITSET TÄMÄN OPPAAN?

Kybermaailma saattaa kuulostaa ilmiöltä, josta vain asiantuntijoiden tulee ymmärtää jotain. Tämä ei pidä paikkaansa, vaan kybermaailma koskee meitä kaikkia. Me kaikki nimittäin elämme arkeamme kybermaailmassa.

Arkemme on viimeisten vuosikymmenien aikana muuttunut erittäin nopeasti, eikä muutoksen tahti osoita hidastumisen merkkejä: päinvastoin. Lähes kaikkiin arkemme asioiden hoitamiseen käytetään nykyisin tietojärjestelmiä, tietoverkkoja ja ohjelmistoja – eli kybermaailmaa.

Hieman yksinkertaistaen voidaan sanoa, että kybermaailmassa on kyse bittien maailmasta. Bitti on tietokoneen ymmärtämässä muodossa olevan tiedon yksikkö, jonka arvo voi olla 1 tai 0. Kybermaailmassa kaikki koostuu biteistä. Tätä voi verrata siihen, että fyysisessä maailmassamme kaikki koostuu atomeista.

Yhä useammin bittien ja atomien maailmat kietoutuvat toisiinsa. Vaikka esimerkiksi televisio on fyysinen esine, ei se toimi ilman bittejä. Aivan samalla tavoin bittien ja atomien yhteispeliä tarvitaan vaikkapa kaupankäynnissä, terveydenhoidossa tai liikenteessä. Tähän liittyen puhutaan nykyisin paljon digitalisaatiosta. Digitalisaatio tarkoittaakin myös bittien maailman ja kybermaailman levittäytymistä yhä laajemmalle kaikkialle elämiimme.

Kybermaailma ja sen bitit siis vaikuttavat meihin kaikkiin, eikä meistä kukaan voi enää jättäytyä kybermaailman ulkopuolelle. Siksi on tärkeää, että me kaikki tiedämme ja ymmärrämme perusasiat kybermaailmasta. Siksi Sinunkin kannattaa lukea tämä opas.

MITÄ TEKEMISTÄ KYBETURVALLISUUDELLA ON ARKEMME KANSSA?

Olemme varmasti kaikki vähintäänkin kuulleet uutisia siitä, kuinka erilaisten tietojärjestelmien toimintahäiriöt ovat vaikuttaneet tavallisten kansalaisten elämään. Ostoksien maksaminen kortilla lähikaupan kassalla ei ole onnistunut, palkka ei ehkä ole tullut tilille ajallaan, tai kaupungin liikenne on ruuhkautunut liikennevalojen ohjausjärjestelmän seottua.

KRIITTINEN INFRASTRUKTUURI

Kriittisellä infrastruktuurilla tarkoitetaan kaikkia niitä palveluita, järjestelmiä ja rakenteita, jotka ovat yhteiskuntamme toiminnalle elintärkeitä. Esimerkkejä kriittisen infrastruktuurin osista ovat mm. maksujärjestelmät, liikenteen ohjausjärjestelmät tai vaikkapa sähköverkko.

KYBERMAAILMA

Kriittinen infrastruktuuri ja kybermaailma ovat nykyään kietoutuneet yhteen niin tiukasti, että useimmissa tapauksissa kriittiseen infrastruktuuriin kuuluvat järjestelmät eivät enää voi toimia, jos kybermaailma ei toimi. Järjestelmille kuuluvien tehtävien suorittamiseen ei useimmiten ole vaihtoehtoisia tapoja. Siksi monet arkemme toiminnot ovat täysin riippuvaisia kybermaailman toimivuudesta.

TURVALLISUUS

Arjen häiriöt ovat ikäviä, ja pahimmassa tapauksessa niistä voi aiheutua myös merkittävää haittaa ja jopa vaaraa. Ennen kaikkea ne rasittavat kuitenkin henkisesti: totuttujen toimintojen ja rutiinien häiriintyminen saattavat horjuttaa turvallisuudentunnetta ja saada meidät epävarmoiksi. Tämä on normaalia, ja onkin hyvä

jo etukäteen pohtia sitä, kuinka selviämme, jos yhteiskuntamme perustoiminnot eivät joskus toimisikaan niin kuin tavallisesti esimerkiksi kybermaailman ongelmien tai jonkin muun syyn vuoksi.

VARAUTUMINEN

Oman selviytymisstrategian pohtimisen avuksi on tarjolla paljon tietoa. Kybermaailmassa esiintyvät vakavat häiriötkin vaikuttaisivat elämäämme hyvin samalla tavoin kuin esimerkiksi laaja sähkökatko. Siksi kannattakin tutustua Puolustusministeriön julkaisemaan oppaaseen ”Pahasti poikki”. Lisäksi kannattaa pitää huoli, että kotona on varastossa kotivara – ruokaa ja muita päivittäin välttämättä tarvittavia tavaroita noin viikon ajaksi. Kotivarasta saat tietoja Suomen Pelastusalan keskusliiton julkaisemasta Kotivara-lehtisestä: WWW.SPEK.FI/KOTIVARA.

MITÄ KYBER TARKOITTAA?

Yksittäisenä sana kyber ei tarkoita mitään, vaan sitä käytetään yhdessä muiden sanojen kanssa. Tyypillisesti kaikki kyber-alkuiset termit viittaavat sähköisessä muodossa olevan informaation käsittelyyn eli tietotekniikkaan, tiedonsiirtoon sekä tietojärjestelmiin.

Kybermaailma vaikuttaa fyysiseen maailmaan ja fyysinen maailma vaikuttaa kybermaailmaan. Yhteys maailmojen välillä on moninainen. Nykyinen yhteiskuntamme toimii bittien varassa. Kybermaailma voidaan nähdä esimerkiksi eräänlaisena kaupunkina.

Kyberkaupunkia ei kuitenkaan ole olemassa kartalla eikä sillä ole maantieteellisiä koordinaatteja. Kyberkaupungissa voimme kuitenkin verkon välityksellä esimerkiksi tavata ihmisiä ja hoitaa päivittäisiä asioitamme. Yritysten toiminta on vilkasta kellonaikaan katsomatta. Kyberkaupunki ei nuku koskaan.

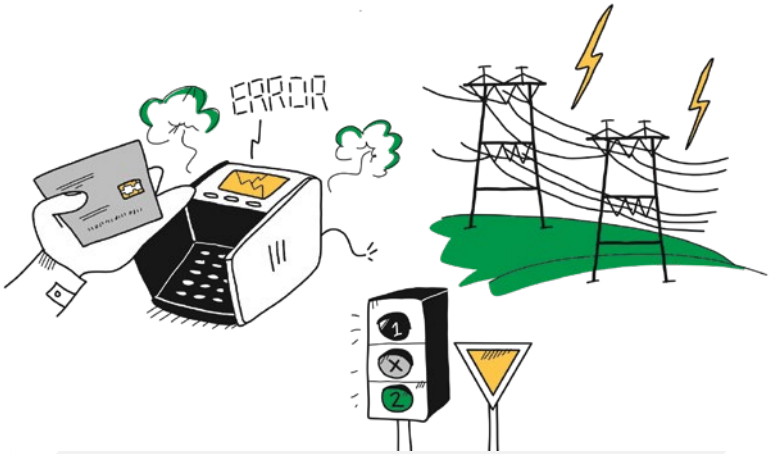
KYBERSANASTO

Kybertoimintaympäristö on digitaalisen informaation käsittelyyn tarkoitettu, toisiinsa yhteydessä olevista tietokoneista ja muista laitteista sekä tietoverkoista muodostunut ympäristö.

Kyberturvallisuus on kybermaailman turvallisuutta. Se tarkoittaa sitä, että erilaiset kybermaailmaan kohdistuvat uhat ovat hallinnassa, ja kybermaailma toimii oikein ja virheettömästi. Tällöin esimerkiksi kybermaailman toimivuudesta riippuvainen kriittinen infrastruktuurikin toimii oikein ja on luotettavaa.

Kyberuhka tarkoittaa mahdollisuutta sellaiseen kybermaailmaan vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa kybermaailman oikean ja virheettömän toiminnan.

Kyberpuolustus on kyberturvallisuuden maanpuolustuksellinen osa-alue. Siihen kuuluvat kybermaailmassa tapahtuva ja sitä koskeva tiedustelu, maanpuolustuksen kannalta merkityksellisten kyberympäristöjen suojaaminen ja tiettyihin kyberympäristöihin vaikuttaminen. Kyberpuolustuksesta vastaa Suomessa Puolustusvoimat.



Informaatiovaikuttaminen on vaikuttamista saatavilla olevan informaation sisältöön ja kulkuun sekä sitä kautta eri vaiheissa olevan tapahtumasarjan lopputulokseen. Tavoitteena voi olla esimerkiksi kansalaisten mielipiteiden muokkaaminen.

IoT (Internet of Things) eli esineiden internet tarkoittaa internetin laajentumista laitteisiin ja koneisiin, joita voidaan ohjata ja mitata verkon kautta. Esineiden internet on yhä useamman arkea: esimerkiksi pesukone voi olla yhteydessä Internetiin.

Kriittinen infrastruktuuri tarkoittaa kaikkia niitä palveluita, järjestelmiä ja rakenteita, jotka ovat yhteiskuntamme toiminnalle elintärkeitä. Esimerkki tästä on sähköverkko.

Palvelunestohyökkäys tarkoittaa verkkohyökkäystä, jossa pyritään estämään tietyn verkkopalvelun tarkoitettu käyttö. Tavallisimmin hyökkäys toteutetaan kohdistamalla palveluun niin paljon verkkoliikennettä, että palvelu ei enää suoriudu tehtävistään.

Phishing eli tietojenkalastelu on toimintaa, jolla pyritään saamaan haltuun luottamuksellisia tietoja (esimerkiksi henkilö- tai tilitietoja) esiintyen tiedon saantiin oikeutettuna tahona. Näiden tietojen avulla voidaan sitten pyrkiä saavuttamaan esimerkiksi taloudellista hyötyä.

Päivitys (ohjelmistopäivitys). Ohjelmistot ovat monimutkaisia, ja niissä onkin käytännössä aina virheitä. Lisäksi ohjelmistoihin saatetaan tarvita uusia ominaisuuksia. Virheitä korjataan ja ominaisuuksia lisätään päivittämällä ohjelmistoja. Päivitys tarkoittaa ohjelmiston muuttamista siten, että aiempi versio korvataan uudella ohjelmistoversiolla.

Tietojärjestelmä on ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoituksena on informaatiota käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi.

Tietoturva viittaa kaikkiin niihin järjestelyihin, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvaan kuuluvat muun muassa tiedon, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Yksilötasolla tietoturva tarkoittaa tärkeiden tietojen ja laitteiden suojaamista.

Trolli on viesti tai henkilö, jonka ensisijainen tavoite on ärsyttää ihmisiä, aiheuttaa ristiriitoja tai aiheuttaa turhien viestien kirjoittamista. Yleensä trollaaja esittää jostakin aiheesta äärimmäisen mielipiteen vastustajien kantaa halventaen ja muiden argumentteja huomioon ottamatta.

Varmuuskopiointi tarkoittaa jonkin tärkeän tiedon kopiointia ja varastointia jonnekin muualle kuin sen alkuperäinen sijainti. Jos alkuperäinen tieto häviää tai tuhoutuu, voidaan tieto palauttaa varmuuskopioista.

MILLAINEN ON HYVÄ SALASANA?

Salasana on hyvä, jos se on riittävän monimutkainen niin, ettei sitä voi arvata tai saada selville kokeilemalla tai laskemalla. Oleellista on kuitenkin myös se, että salasanan muistaa. Kuinka siis keksiä hyvä salasana?

Salasanan sijaan kannattaakin keksiä salalause – salasanassa kun pidempi on aina parempi, ja kun lauseen on itse keksinyt, sen myös muistaa. Lisäturvaa tuo se, että käytät vaikkapa murresanoja tai muuten harvinaisempia sanoja ja lisäät mukaan erikoismerkkejä ja numeroita.

Siis esimerkiksi näin: KahtooKunKissa2UuttaKonttie!

Salasanassa voi siis käyttää kirjaimia numeroita ja erikoismerkkejä, mutta ei kirjaimia å, ä ja ö. Kaikissa palveluissa kannattaa käyttää eri salasanaa. Salasanojen hallintaan on saatavilla myös ohjelmia, joihin voi kerätä kaikki salasanansa.

ENTÄ MITÄ ON INFORMAATIOVAIKUTTAMINEN?

Sanotaan, että tieto on valtaa. Siksi tietoon – eli informaatioon – pyritäänkin vaikuttamaan koko ajan. Arjessamme esimerkkejä tällaisesta vaikuttamisesta ovat mm. mainonta tai valistuskampanjat, joilla meitä yritetään saada syömään terveellisemmin tai liikkumaan enemmän.

Tietoon vaikuttaminen on merkittävä osa myös valtioiden välisiä suhteita ja erilaisia kriisejä. Tällaisissa tapauksissa puhutaan informaatiovaikuttamisesta tai informaatiosodankäynnistä. Niillä tarkoitetaan vaikuttamista kansalaisiin, päätöksentekijöihin ja toimintakykyyn ohjailemalla saatavilla olevaa informaatiota ja sen kulkua.

TEKNOLOGIA

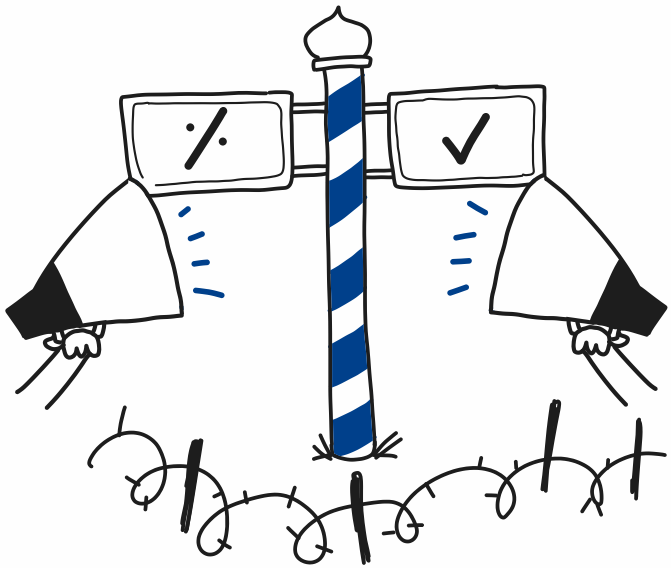
Teknologia on muuttanut suomalaistakin viestintäympäristöä huomattavasti. Perinteisellä medialla ei ole enää pitkään aikaan ollut viestinnällistä monopolia, vaan kuka tahansa voi saavuttaa hyvinkin suuria yleisöjä internetin ja sosiaalisen median kautta. Siksi informaatiovaikuttaminenkin on nykyisin helpompaa – ja usein huomaamattomampaa – kuin aiemmin.

KYSEENALAISTAMINEN

On tärkeää, ettemme kyseenalaistamatta usko kaikkea, mitä esimerkiksi sosiaalisessa mediassa näemme. Siellä välitettävä tieto voi olla tahallisesti vääristeltyä tai täysin virheellistä. On olemassa jopa kokonaisia verkkosivustoja, joiden tarkoituksena on levittää virheellistä ja jonkin tietyn toimijan etuja palvelevaa tietoa. Tällöin voidaan puhua valemediasta – oikeat mediat tarkistavat välittämänsä tiedot ja pyrkivät aina mahdollisimman virheettömään viestintään, vaikka niilläkin toki on usein omia tavoitteita ja tarkoitusperiä.

OSAAMINEN + TIETO = SUOJAUTUMINEN

Informaatiovaikuttamiselta suojautuminen perustuu osaamiseen ja tietoon. Informaation lähdettä kannattaa aina pyrkiä arvioimaan sitä koskevan tiedon perusteella ja samasta aiheesta kannattaa pyrkiä hankkimaan tietoa useista eri lähteistä. Tällöin voi kehittää ns. media- tai monilukutaitoaan, joka on yksi modernin yhteiskunnan uusista kansalaistaidoista.



MITEN KYBERTURVALLISUUS VAIKUTTAA JUURI MINUUN?

Kun puhumme kyberturvallisuudesta, voimme puhua myös tietoturvasta. Jokaisen digitaalinen identiteetti – esimerkiksi pankkitunnukset ja eri palveluiden salasanat – ovat sellaista tietoa, joka kannattaa ja jonka haluamme turvata. Tähän voimme itse vaikuttaa esimerkiksi pitämällä erilaiset laitteet ja niiden ohjelmistot päivitettyinä sekä käyttämällä virustorjuntaohjelmia ja eri salasanoja eri palveluihin.

Toisaalta on myös paljon sellaisia asioita joihin emme voi vaikuttaa, mutta joiden ymmärtäminen on tärkeää. Arjessamme moni asia on kytkeytynyt verkottuneeseen yhteiskuntaan. Vesi tulee hanasta ja sähkö pistorasiasta, mutta niin ei tapahdu ilman kybermaailmaa. Erilaiset toiminnot ovat hyvin riippuvaisia kybermaailman toimivuudesta.

Maalaisjärjellä pääsee pitkälle. Usein sellainen asia, joka kuulostaa liian hyvälle ollakseen totta ei olekaan totta. Oppaan viimeisellä sivulla on kymmenen ja yksi kansalaisen kyberkäskyä, joiden avulla parannat omaa ja myös muiden kyberturvallisuutta.

HALUATKO TIETÄÄ LISÄÄ?

Kiinnostuitko kyberturvallisuudesta, ja haluaisitko tietää ja oppia sitä lisää? Tämän oppaan julkaisseet Maanpuolustuskoulutusyhdistys (MPK) ja Jyväskylän yliopisto järjestävät molemmat kaikille avointa koulutusta kyberturvallisuuteen liittyen. Saat tarjolla olevasta koulutuksesta tietoa verkosta osoitteista WWW.MPK.FI/KOULUTUS ja WWW.JYU.FI/IT/KYBER. Tervetuloa!

TEKSTI

Irina Lönnqvist (MPK)
Panu Moilanen (JY)

KUVITUS

Linda Saukko-Rauta
Redanredan Oy, 2017

TAITTO

Ossi Hietala

JULKAISIJAT

Jyväskylän yliopisto 2018
Maanpuolustuskoulutus-yhdistys 2018

PAINO

Jyväskylä/Rauma

ISBN

978-951-39-7588-3
(nid., 2. korjattu painos)
978-951-39-7589-0
(verkkoj., 2. korjattu painos)

MAHDOLLISTAJA

ICT-Suomi ry

MPK
MAANPUOLUSTUSKOULUTUSYHDISTYS
FÖRSVARSUTBILDNINGSFÖRENINGEN

JYU. Since 1863.

ICT SUOMI

KANSALAISEN 10+1 KYBERKÄSKYÄ

1 Ole terveen epäluuloinen ja kysy riittävän usein miksi.

2 Mieti aina, mitä laitat verkkoon: kaikkea ei tarvitse kertoa ja kerran verkkoon laitettua ei saa sieltä enää pois.

3 Varmista klikkaamasi linkin tai Sinulle lähetetyn liitetiedoston aitous – jos vähänkin epäilyttää, ole yhteydessä esimerkiksi viestin lähettäjään.

4 Huolehdi kaikkien laitteidesi päivityksestä ja tietoturvasta. Jos et itse osaa, kysy neuvoa esimerkiksi tuttavilta tai tukipalvelusta. Tietoturva on väärä kohta säästää. Ole varovainen, jos käytät jotain muuta kuin omaa laitettasi.

5 Ole raha-asioiden – esimerkiksi luottokortti- ja verkkopankkitietojen – kanssa erityisen tarkka. Älä luovuta henkilökohtaisia tietojasi, jos et ole aivan varma, kenelle olet niitä luovuttamassa.

6 Muista, että julkiset ja avoimet langattomat verkot ovat turvattomia.

7 Muista varmuuskopiointi.

8 Käytä riittävän hyviä salasanoja.

9 Jos jokin kuulostaa liian hyvältä ollakseen totta, se ei yleensä ole totta.

10 Kybermaailman tarjoamat hyödyt ovat suurempia kuin haitat: älä pelkää turhaan!

+1 Huolehdithan mahdollisuuksien mukaan myös muiden – esimerkiksi lastesi ja vanhempiesi – osaamisesta ja tietoturvasta.