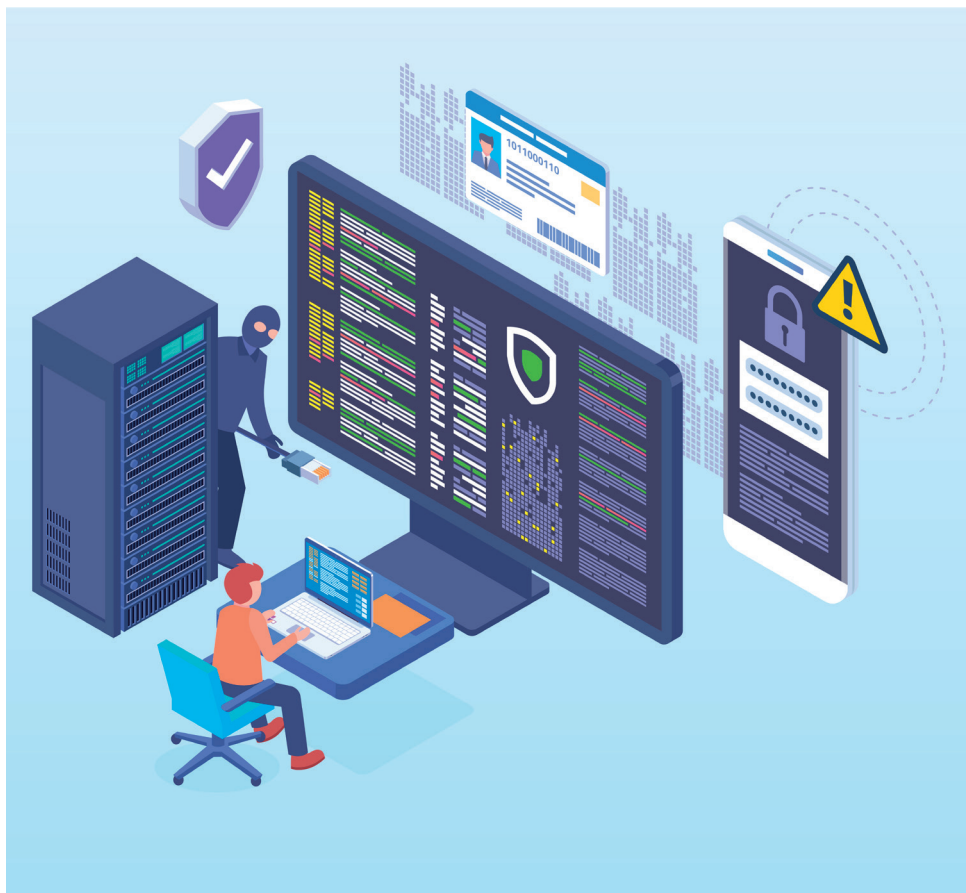


Yrityksiin kohdistuva hybridivaikuttaminen

KESÄKUU 2022

SELVITYS



KESKUS-
KAUPPAKAMARI



HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

SISÄLTÖ

JOHDANTO	4
YRITYKSET HYBRIDIVAIKUTTAMISEN KOHTEINA	7
YRITYSTEN VARAUTUMINEN HYBRIDIVAIKUTTAMISEEN.....	15
RIKOLLISUUDEN JA HYBRIDIVAIKUTTAMISEN SEURAUKSET	25
YRITYSTEN ODOTUKSET VIRANOMAISILTA JA YHTEISTYÖ	31
YRITYSTEN KYKY KESTÄÄ ERI RESURSSIEN SAATAVUUDEN HÄIRIÖITÄ.....	37
JOHTOPÄÄTÖKSET.....	46
LISÄTIETOA	50



Lisätietoja:

Panu Vesterinen
Hankejohtaja
Lujat-kehityshanke
panu.vesterinen@chamber.fi

**KESKUS-
KAUPPAKAMARI**



HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

JOHDANTO

Yrityksiin kohdistuva hybridivaikuttaminen 2022 –selvityksen tavoitteena on kartoittaa miten yritykset ymmärtävät hybridiuhat, millainen ilmiö ne ovat, miten ne kohdistuvat yrityksiin ja miten yritykset ovat osanneet varautua niiden varalta.

Hybridivaikuttaminen ja yritykset

Hybridivaikuttaminen tarkoittaa nimensä mukaisesti useamman kuin yhden keinon käyttämistä tavoiteltaessa haluttua lopputulosta. Yritys voi olla lopullinen kohde, mutta todennäköisempää on että sitä käytetään reittinä tai välikappaleena lopulliseen tavoitteeseen pyrittäessä. Hybridivaikuttamisen keinoja on vaikea luetella tyhjentävästi, koska vaikuttamiseen pyrkivä taho voi kohteesta ja tavoitteesta riippuen käyttää täysin ennalta-arvaamattomia keinoja.

Hybridivaikuttamisoperaatiot voivat olla hyvinkin pitkäaikaisia, niiden valmistelu, yhteyksien ja vaikutusvallan hankkiminen voi kestää useita vuosia. Myös hyväksikäytettävä tieto on kerätty vuosien aikana vieraan valtion palkkalistoilla olevien henkilöiden toimesta, perinteisin vakoilun keinoin tai sitten digitaalista toimintaa hyväksikäyttäen.

Hybridivaikuttaminen voi olla taloudellista tai poliittista vaikuttamista ja sen keinot voivat olla erilaisia kuten disinformaatiokampanjat, vaikutusaseman hankkiminen sijoittamalla rahaa liiketoimintaan tai politiikkaan ja viimekädessä valtioiden väliset taloudelliset sanktiot. Vaikuttamista voidaan kohdistaa poliittiseen päätöksentekoon, viranomaisten toimintaan ja yritys-toimintaan tai kaikkiin samanaikaisesti.

Yrityksiin liittyvänä tavoitteena voi olla kriittiseen infrastruktuuriin liittyvien yritysten toimintaan mukaan pääseminen tai vaikutusvallan hankkiminen yrityskauppojen tai kaupallisen yhteistyön kautta. Yrityksiin kohdistuva hybridivaikuttamisoperaatio muistuttaa ulkoisesti tavallista yritystoimintaa, mutta sitä ohjaa vieraan vallan tavoite vaikuttaa johonkin asiaan. Suurusluokaltaan vaikuttamista voi suurimmillaan olla kriittisen infran miljardihanke

ja pienimillään yksittäisen politiikan tai valmistelevan virkamiehen ohjailu jonkin halutun tavoitteen saavuttamiseksi.

Yritysten rooli suomalaisen yhteiskunnan suojaamisessa on merkittävä. Toimiva yhteistyö viranomaisten kanssa luo vahvan pohjan hybridivaikuttamisen tunnistamiseksi ja sen seurausten torjumiseksi.

Selvitys on osa Keskuskauppakamarin ja Huoltovarmuuskeskuksen LUJAT -hanketta. Koko Suomessa kauppakamareilla on yli 21000 jäsenyrtystä.

Tutkimuksen toteuttaminen ja vastaajien taustatiedot

Selvitys käsittelee suomalaisten yritysten käsityksiä niihin kohdistuvista hybridihista ja niihin varautumisesta. Selvitys perustuu 277 suomalaisen yrityksen antamiin vastauksiin.

Taloustutkimus toteutti kyselyn Keskuskauppakamarin toimeksiannosta. Yritykset vastasivat kyselyyn maaliskuussa 2022. Tutkimustulokset on esitetty taulukoina ja kuvioina, joista yksittäisen vastaajan mielipide ei käy ilmi.

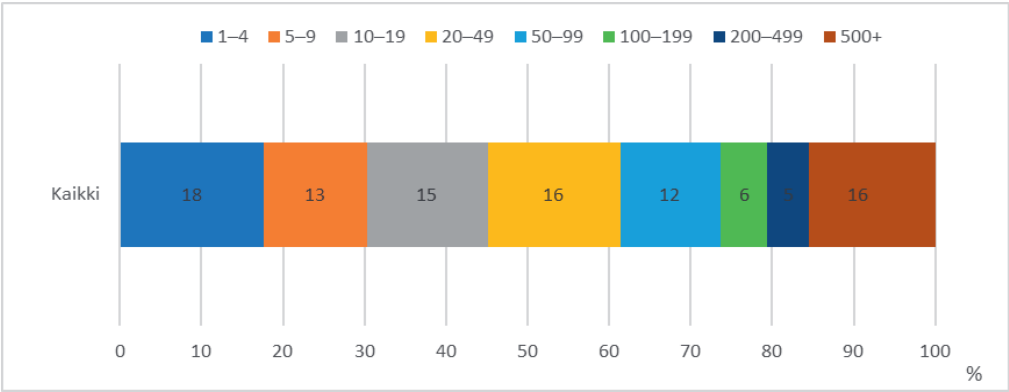
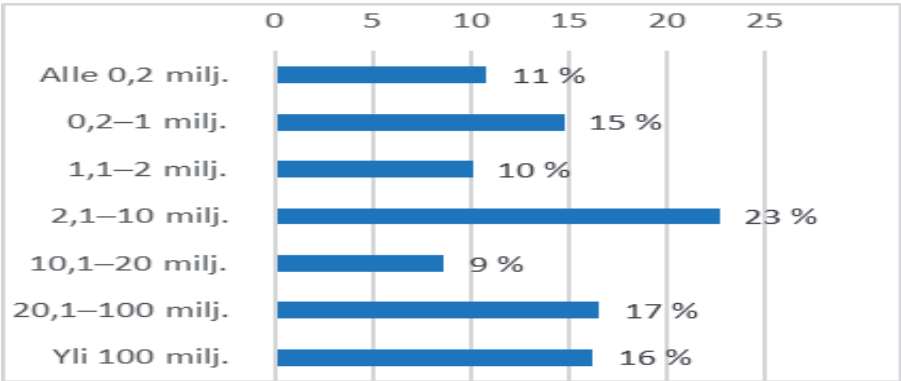
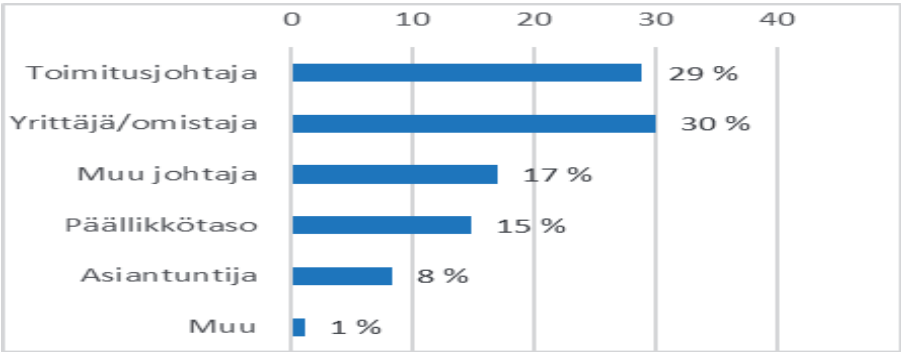
Selvityksen on laatinut hankejohtaja Panu Vesterinen. Selvitys on osa Keskuskauppakamarin LUJAT -hanketta.

Vastanneista yrityksistä 60 % on henkilömäärältään pieniä yrityksiä, jotka työllistävät alle 50 henkilöä. Vastaajista 18 % on keskisuuria yrityksiä, joiden palveluksessa on 50–200 työntekijää. Suuria yrityksiä, jotka työllistävät yli 200 henkilöä, oli 21 % kaikista vastaajista.

Vastaajat olivat yritysten toimitusjohtajia (29 %), yrittäjiä tai omistajia (30 %), muita johtajia (17 %). Kahdeksan prosenttia vastaajista oli asiantuntijatehtävissä. Pääliikötason tehtävissä vastaajista oli viisitoista prosenttia. Vastaajien rakenne kertoo siitä että tutkimus on tavoittanut erityisesti yritysten päätöksentekijät.

Keskuskauppakamari kiittää vastaajia luottamuksesta, jonka osoituksena on runsas avoimien vastausten määrä. Osa näistä avoimista vastauksista on liitetty tiettyjen lukujen viimeiseksi osioksi. Lainaukset on korostettu petiitti -fontilla ja erotettu lainausmerkeillä. Ne sisältävät hyviä herätteitä ja esimerkkejä aihealueesta.

Selvityksen lähdeluetteloon on koottu lisätietoa hybridiuhista yritysten turvallisuus toiminnan tueksi.



YRITYKSET HYBRIDIVAIKUTTAMISEN KOHTEINA

Yhteiskuntaan ja yrityksiin kohdistuu jatkuvasti erilaista vaikuttamista. Vain murto-osa siitä on vieraan valtion päämääriä ja tarkoituseriä palvelevaa vaikuttamista. Yritystoiminnassa on helppoa peittää vaikuttaminen ja saada sen tarkoituksena piilotettua normaalilta vaikuttavan yritystoiminnan taakse. Yrityksillä on merkittävä rooli osana yhteiskunnan resilienssiä. Yrityksiin kohdistuvan ja niitä hyödyntävän hybridivaikuttamisen nostaminen julkisuu-teen tällaisen selvityksen kautta on tärkeää.

Yritys ei voi kokonsa puolesta vetää sitä johtopäätöstä ettei se voisi olla vaikuttamisen kohde tai reitti. Avainasemassa vieraan valtion kannalta usein on se, millaisia yhteyksiä ja asiakkuuksia yrityksellä on. Vakoilun tapaan toimet määräytyvät kohteen mukaan. Hybridivaikuttamisessa voidaan käyttää vuosien aikana eri lähteistä kerättyä tietoa ihmisistä, heidän kon-takteistaan ja heikkouksistaan. Yrityksen johdon tulisi hyväksyä ajatus siitä, että yritys saattaa joutua rikollisen toiminnan kohteeksi. Ja sen jälkeen kehittää kouluttamalla ja ohjeistamalla yrityksen rikos- ja tietoturvasuutta ja turvallisuusmyönteistä yrityskulttuuria. Tällä tavoin yritys varautuu myös hybridivaikuttamisen varalle.

Yritykseen kohdistuvan vaikuttamisen tai hybridivaikuttamisen syyt

Hybridivaikuttaminen tarkoittaa nimensä mukaisesti useamman kuin yhden keinon käyttämistä tavoiteltaessa haluttua lopputulosta. Yritys voi olla lo-pullinen kohde, mutta todennäköisempää on että sitä käytetään reittinä tai välikappaleena lopulliseen tavoitteeseen pyrittäessä. Hybridivaikuttamisen keinoja on vaikea luetella tyhjentävästi, koska vaikuttamiseen pyrkivä taho voi kohteesta ja tavoitteesta riippuen käyttää täysin ennalta-arvaamatto-mia keinoja.

Hybridivaikuttamisoperaatiot voivat olla hyvinkin pitkäaikaisia, niiden valmistelu, yhteyksien ja vaikutusvallan hankkiminen voi kestää useita vuosia. Myös hyväksikäytettävä tieto on kerätty vuosien aikana vieraan valtion palkkalistoilla olevien henkilöiden toimesta, perinteisin vakoilun keinoin tai sitten digitaalista toimintaa hyväksikäyttäen.

Hybridivaikuttaminen voi olla taloudellista tai poliittista vaikuttamista ja sen keinot voivat olla erilaisia kuten disinformaatiokampanjat, vaikutusaseman hankkiminen sijoittamalla rahaa liiketoimintaan tai politiikkaan ja viimekädessä valtioiden väliset taloudelliset sanktiot. Vaikuttamista voidaan kohdistaa poliittiseen päätöksentekoon, viranomaisten toimintaan ja yritystoimintaan tai kaikkiin samanaikaisesti.

Yrityksiin liittyvänä tavoitteena voi olla kriittiseen infrastruktuuriin liittyvien yritysten toimintaan mukaan pääseminen tai vaikutusvallan hankkiminen yritys-kauppojen tai kaupallisen yhteistyön kautta. Yrityksiin kohdistuva hybridivaikuttamisoperaatio muistuttaa ulkoisesti tavallista yritystoimintaa, mutta sitä ohjaa vieraan vallan tavoite vaikuttaa johonkin asiaan. Suurusluokaltaan vaikuttamista voi suurimmillaan olla kriittisen infran miljardihanke

Kaikkien vastaajayritysten keskuudessa myös seuraavia kolmea syytä pidettiin merkittävänä:

- Asiakassuhteet kansallisten turvallisuuteen liittyvien viranomaisten kanssa (19 %)
- Työntekijät, joilla on paljon seuraajia sosiaalisessa mediassa (19 %)
- Aktiivinen jäsenyys ja toiminta vaikutusvaltaisissa liike-elämän järjestöissä (16 %)

Suurien vastaajayritysten osalta esille nousivat seuraavat syyt joutua vaikuttamisen kohteeksi:

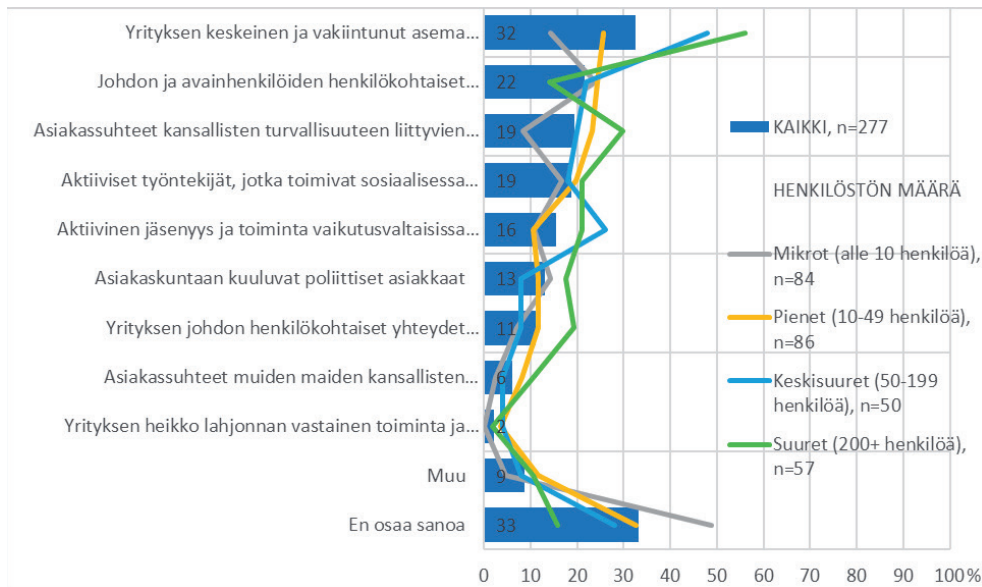
- Keskeinen ja vakiintunut asema suomalaisessa yhteiskunnassa (46 %)
- Asiakassuhteet kansallisen turvallisuuteen liittyvien viranomaisten kanssa (30 %)
- Työntekijät, joilla on paljon seuraajia sosiaalisessa mediassa (22 %)
- Aktiivinen jäsenyys ja toiminta vaikutusvaltaisissa liike-elämän järjestöissä (21 %)
- Johdon henkilökohtaiset yhteydet poliitikkoihin (45 %)

Keskikokoisten vastaajien osalta:

- Keskeinen ja vakiintunut asema suomalaisessa yhteiskunnassa (56 %)
- Aktiivinen jäsenyys ja toiminta vaikutusvaltaisissa liike-elämän järjestöissä (26 %)
- Johdon ja avainhenkilöiden yhteydet johtaviin ja toteuttavan tason virkamiehiin (22 %)
- Asiakassuhteet kansallisen turvallisuuteen liittyvien viranomaisten kanssa (20 %)

-Aktiiviset työntekijät sosiaalisessa mediassa (19 %)

Mitkä ovat mielestänne kolme todennäköisintä syytä, joiden vuoksi yritykseenne kohdistuisi toimintaa, jonka lopullisena tarkoituksena olisi vaikuttaa suomalaiseen tai muun maan yhteiskuntaan, väestöön tai hallintoon?



Yritysten heikkoudet joiden kautta ulkomaiset tahot pyrkivät vaikuttamaan

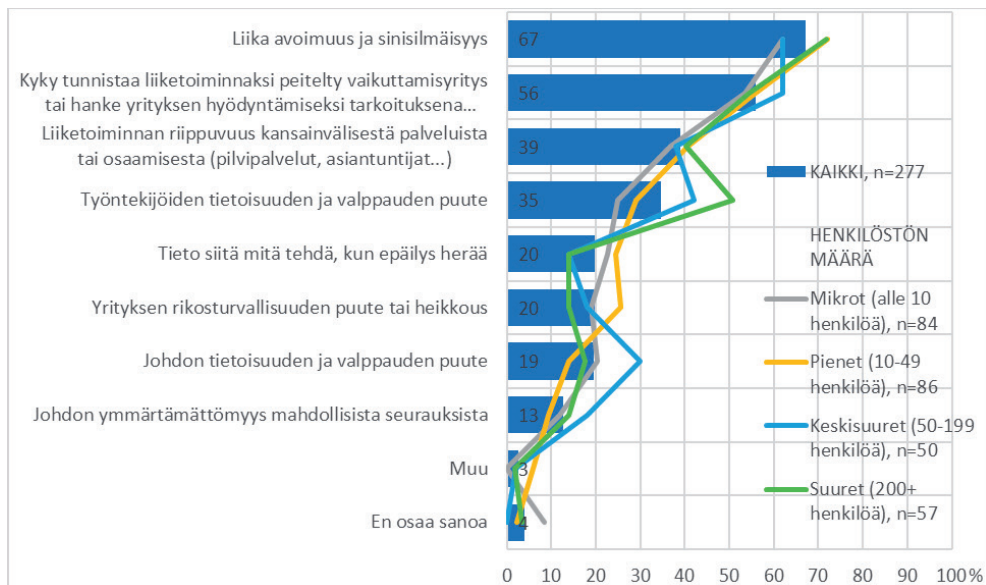
Neljä merkittävintä suomalaisten yritysten heikkoutta vaikuttamisen suhteen ovat liika avoimuus ja sinisilmäisyys (67 %), kyky tunnistaa liiketoiminnaksi peitelty vaikuttamisyritys tai hanke yrityksen hyödyntämiseksi tarkoituksena vaikuttaa varsinaiseen kohteeseen (56 %), liika riippuvuus kansainvälisistä palveluista tai osaamisesta (39 %) ja työntekijöiden tietoisuuden ja valppauden puute (35 %).

Valtiolliset tiedustelu- ja turvallisuuspalvelut tekevät pitkäjänteistä työtä vuodesta toiseen. Ne keräävät tietoa, jota voidaan hyödyntää myöhemmin tai sitten ne keräävät jotain määriteltyä tietoa tietystä kohteesta. Niillä on osaamista ja kokemusta löytää eri kohteiden heikkoudet, joita voidaan hyödyntää kulloisenkin

tavoitteen saavuttamiseksi. Vuosia sitten hankittu tieto voi muuttua arvokkaaksi, mikäli siihen liittyvä henkilö etenee urallaan tehtävään jossa hänestä voi olla hyötyä tavalla tai toisella. Yritysten kannalta jatkuva työntekijöiden ja yrityksen tietojen suojaaminen, henkilökunnan kouluttaminen, valppautta ylläpitävän tiedon jakaminen henkilökunnalle ja rikos- ja tietoturvallisuuden kehittäminen ovat ensisijaisia toimia vakoilua ja vaikuttamista vastaan.

Johdon tietoisuuden ja valppauden puute korostui keskisuurissa yrityksissä (30 %). Suurten vastaajayritysten keskuudessa puolet (51 %) piti heikkoutena työntekijöiden tietoisuuden ja valppauden puutetta.

Mitkä ovat kolme merkittävintä suomalaisten yritysten heikkoutta, kun arvioidaan ulkomaisten toimijoiden (rikollisten tai valtioiden) pyrkimyksiä vaikuttaa liiketoiminnan kautta?



Rikollisten tai ulkomaisten valtion toimijoiden vaikuttamisen todennäköisyys

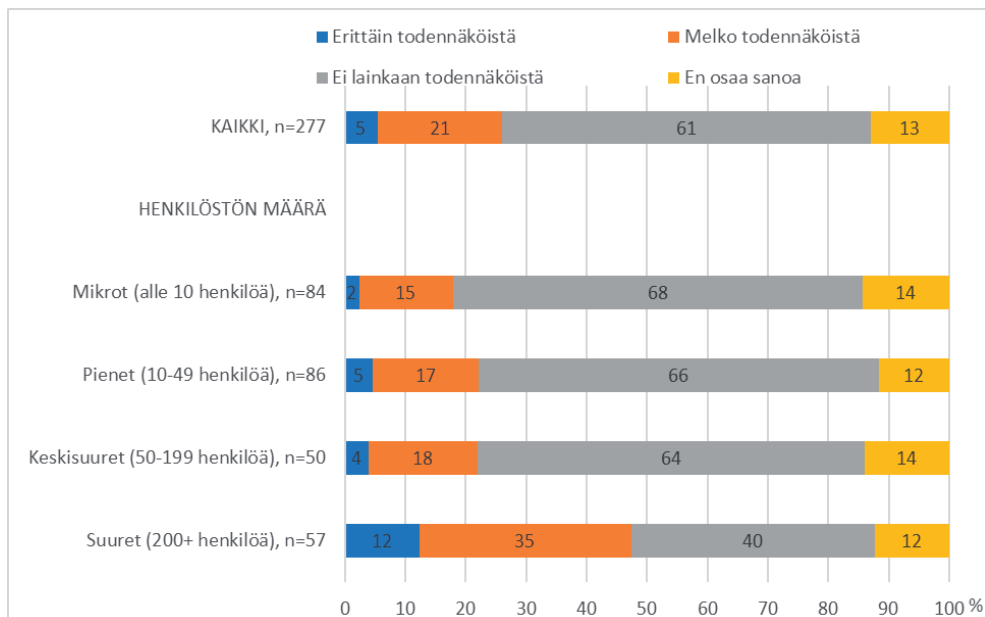
Neljäsosa vastaajista (26 %) piti vähintään melko todennäköisenä että rikolliset tai ulkomaiset valtiolliset toimijat voisivat kohdistaa niihin vaikuttamista.

Kaksi kolmasosaa yrityksistä (61 %) ei pitänyt vaikuttamista todennäköisenä. Tämä on linjassa sen kanssa ettei suurin osa yrityksistä ole potentiaalisia kohteita vaikuttamiselle. Joissain tilanteissa tosin pienikin yritys tai sen johtoon kuuluva voi olla kohteena virkamiesyhteyksien, poliittisten suhteiden tai asiakkuuksien takia.

Puolet suurista yrityksistä (47 %) arvioi tämän olevan vähintään melko todennäköistä. Suuret yritykset ovat näkyviä, niillä on usein laaja asiakaskunta, valtiollisia asiakkaita, suhteita poliitikkoihin, yhteiskunnan infraan liittyviä toimeksiantoja ja muita vastavia tekijöitä joiden kautta ne voivat valikoitua vaikuttamisen kohteiksi tai reiteiksi lopullisiin kohteisiin. Keskiuurista vastaajista viidesosa (22 %) piti tätä vähintään melko todennäköisenä.

Aiemmin vuonna 2018 toteutetussa selvityksessä vain kaksi prosenttia suurista vastaajayrityksistä piti vaikuttamisen mahdollisuutta erittäin todennäköisenä. Tässä selvityksessä määrä oli kasvanut kymmenen prosenttiyksikköä 12 prosenttiin. Vaikuttamista ja sen eri keinoja on viime vuosen aikana käsitelty laajasti julkisuudessa. Osaltaan tämä on oletettavasti nostanut erityisesti suurten yritysten tietoisuutta mahdollisuudesta olla vieraan valtion kohteena tavalla tai toisella.

Kuinka todennäköistä mielestänne on, että rikolliset tai ulkomaiset valtion toimijat voisivat kohdistaa yritykseenne toimintaa, jonka lopullisena tarkoituksena on vaikuttaa Suomen sisäiseen vakauteen, talouteen, ulko- ja turvallisuuspolitiikkaan tai hallituksen toimintaan?



Rikollisten tai ulkomaisten tiedustelupalvelujen pääsy yrityksen tietoihin

Kyberrikollisuus ja kyberuhkien laajuus ja vaikuttavuus ovat olleet yleisessä tiedossa jo vuosien ajan. Yritykset osaavat pitää niitä todennäköisinä riskeinä. Kybertoiminta on nopeaa eikä vaadi aina suuria kustannuksia. Kiinnijäämisen riski on häviävän pieni. Muut keinot vievät huomattavasti enemmän aikaa ja niiden toteutus vaatii kärsivällisyyttä ja läsnäoloa kohdemaassa. Vaikuttamisessa on kuitenkin kyse valtion toiminnasta ja valtioilla on resursseja ja aikaa kehittää toimintaa vuosien ajan. Joidenkin valtioiden vakoilubudjetti on suurempi kuin Suomen valtion budjetti. Siksi perinteistä henkilötiedustelua ja värvättyjen henkilöiden käyttöä ei tule väheksyä.

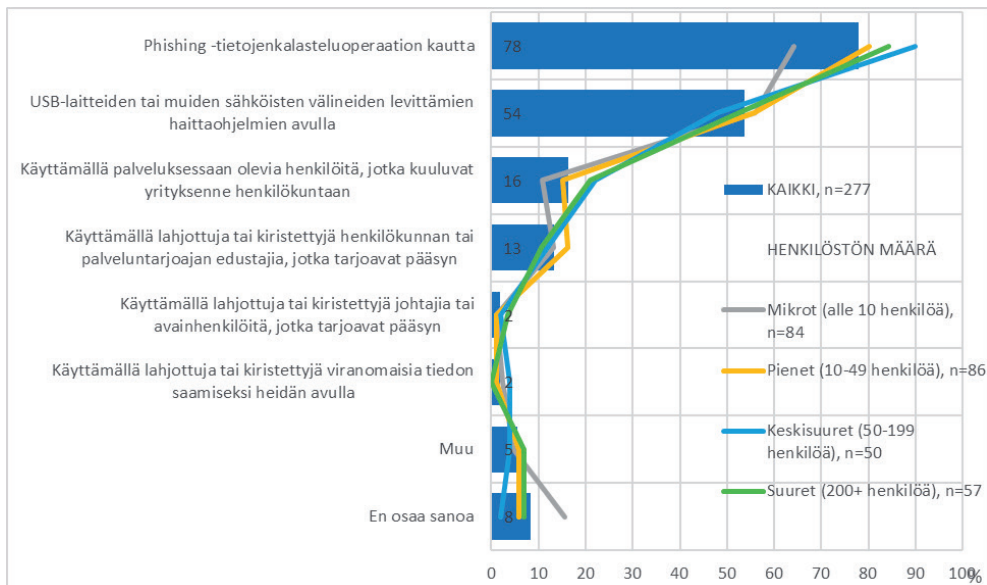
Kaikkea tietoa ei tavoiteta kybervakoilun keinoin tai kaikkea sabotaasien valmistelua ei voida toteuttaa kybertoiminnan kautta. Sen vuoksi henkilöiden käyttäminen vaikuttamistoiminnassa ei ole poissuljettua eikä harvinaista. Houkuttelevana kohteena voidaan pitää poliitikkoja, virkamiehiä tai yritys-elämän edustajia, jotka esiintyvät julkisuudessa tuoden esille haluttuja mielipiteitä vaikuttaen yleisiin mielipiteeseen asioista tai heikentäen luottamusta yhteiskuntaan.

Rikollisten tai ulkomaisten tiedustelupalveluiden uskotaan pääsevän kohteeksi valitsemansa yrityksen tietoihin yleisimmin phishing –tietojenkalasteluoperaation kautta (78 %) ja USB-laitteiden tai muiden sähköisten välineiden levittäminen haittaohjelmien avulla (51 %).

Phishing-tietojenkalastelu nousi selkeästi esille suurten yritysten (84 %) ja keski-suurten yritysten (90 %) keskuudessa.

Seuraavaksi yleisimpinä keinoina pidettiin vaikuttajan palveluksessa olevia henkilöitä jotka kuuluvat kohteen henkilökuntaan (16 %) ja lahjottuja kohteen työntekijöitä tai sen palveluntarjoajan edustajia (13 %).

Miten uskotte rikollisten tai ulkomaisten tiedustelupalvelujen pääsevän kohteekseen valitsemansa yrityksen tietoihin? Valitse kaksi todennäköisintä vaihtoehtoa.



”Asiakassuhteet yrityksiin, jotka toimivat turvallisuuteen liittyvien viranomaisten kanssa – olemme osa toimitusketjua.”

”Maantieteellinen sijainti ja rooli sijaintialueen infrastruktuurin ylläpitäjänä.”

”Toiminta kansalliseen turvallisuuteen liittyvissä hankkeissa eri rooleissa.”

”Toimiminen huoltovarmuuskriittisellä toimialalla (energia-ala).”

”Henkilöt, työntekijät ja toimijat, joiden motiivit toimia perustuvat ulkoa ohjattuun ja (pitkäaikaiseen) suunnitelmalliseen toimintaan.”

”Tiedonkalastelu yritys, minkä olemme venäläiseltä (suomalaisten omistamalta) yritykseltä saaneet viime vuonna oli selkeä yritys kartoittaa maatamme täysin tarpeettoman ”sertifioinnin” avulla.”

”Olemme tilitoimisto hoidetaan useiden eri yritysten taloushallintoa. Maksuliikennettä ja tiedetään paljon yrityksistä ja ihmisistä. On jopa ruvennut pelottamaan tänä tiedon määrää.”

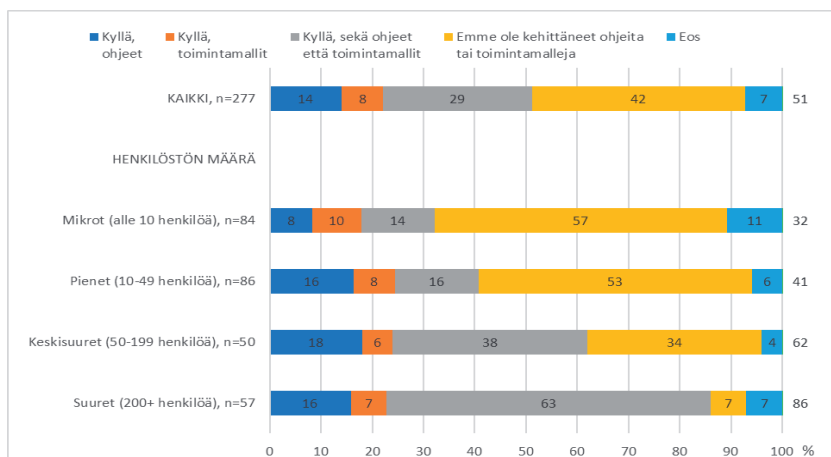
YRITYSTEN VARAUTUMINEN HYBRIDIVAIKUTTAMISEEN

Yritykset voivat varautua hybridivaikuttamiseen normaalilla yritysturvallisuuden keinovalikoimalla. Näitä ovat yritysturvallisuuden ylläpitäminen, erityisesti rikos- ja tietoturvallisuuden kehittäminen, henkilöstön kouluttaminen, tiedonvaihto viranomaisten ja yritysten kesken, tiedonjako henkilökunnalle ja johdon sitoutuminen niihin.

Ohjeet tai toimintamallit riskien varalle

Puolella vastaajista (51 %) on käytössä ohjeet, toimintamallit tai molemmat. Keskiuurilla yrityksillä on joko ohjeet tai toimintamallit tai molemmat (62 %). Suurten vastaajien keskuudessa vastaava prosentti on korkein (86%). Lähes puolet kaikista vastaajista (42 %) ei ole ohjeita tai toimintamalleja yrityksen suojaamiseksi. Monessa yritykseen kohdistuvan toiminnan tunnistamisessa ratkaisevassa asemassa on työntekijöiden yleinen turvallisuusvalppaus, jota voidaan kehittää jakamalla tietoa, kouluttamalla ja rakentamalla pitkäjänteisesti turvallisuusmyönteistä yrityskulttuuria.

Oletteko kehittäneet ohjeet tai toimintamalleja edellä mainittujen riskien varalle?

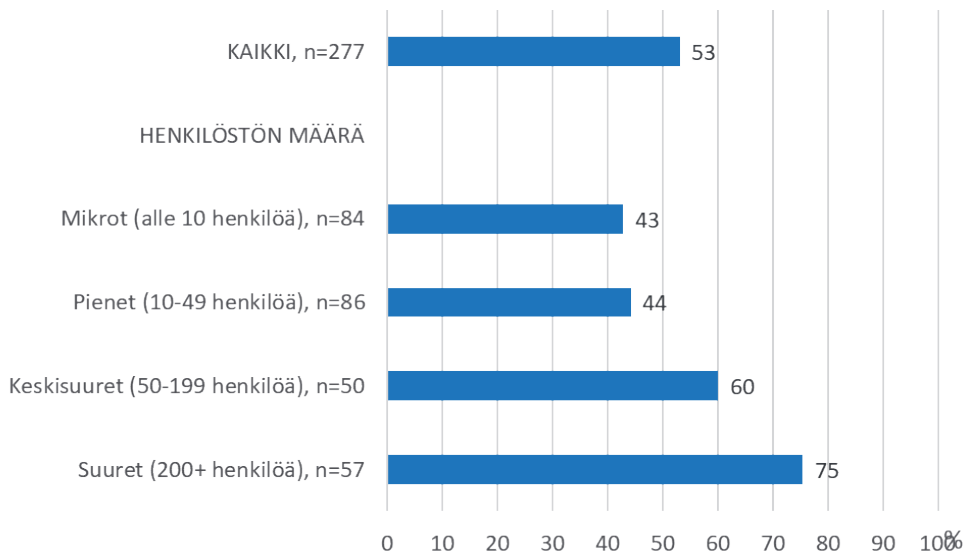


Ohjeet urkkimisen tunnistamiseksi ja tiedon suojaamiseksi

Puolet vastaajayrityksistä (53 %) on laatinut ohjeet urkkimisen tunnistamiseksi ja tiedon suojaamiseksi. Yleisintä se on suurten yritysten (75 %) keskuudessa. Keskisuurista noin kaksi kolmasosaa (60 %), pienistä hieman alle puolet (44 %) ja mikroyrityksistä 43 prosenttia on laatinut ohjeen.

Tiedon luokittelu on tiedon suojaamisen perusta, ilman sitä on vaikea tietää mitä pitää suojata ja kenellä on tarve saada pääsy tietoon. Vieras valtio voi käyttää monenlaista tietoa eri tavoin hyväkseen. Tiedon avulla voi esimerkiksi löytää värväämiseen sopivia työntekijöitä, saada tietoa kriittisen infrastruktuurin kohteiden turvallisuusjärjestelyistä, suunnitelluista hankkeista, asiakkuuksista, yrityksen taloustilanteesta, yrityssalaisuuksista ja suhteista poliittikoihin tai virkamiehiin.

Onko yrityksellänne ohjeistusta, jolla auttaa työntekijää tunnistamaan tiedon urkkimisyrityksen ja jolla yritätte estää työntekijän luovuttamasta vahingossa tietoa sitä urkkiville tahoille?



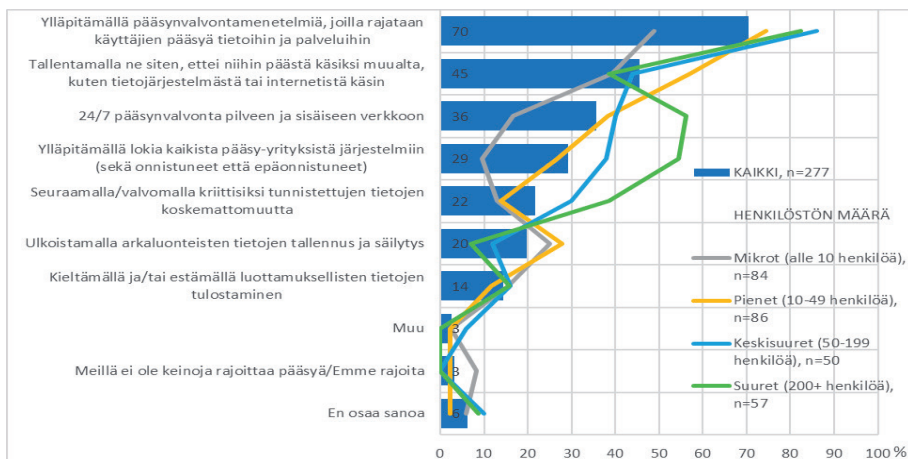
Pääsyn rajoitus tärkeisiin ja/tai luottamuksellisiin yritystietoihin

Yleisimmin käytössä oleva keino rajoittaa pääsyä tärkeisiin tai luottamuksellisiin yritystietoihin oli ylläpitää pääsynvalvontamenetelmiä, joilla rajataan käyttäjien pääsyn tietoihin ja palveluihin (70 %). Toiseksi yleisin tapa (45 %) oli rajoittaa tärkeisiin ja/tai luottamuksellisiin yritystietoihin pääsyä tallentamalla ne siten, ettei niihin pääse käsiksi tietojärjestelmästä tai internetistä käsin. Kolmanneksi yleisin tapa (36 %) oli ylläpitää 24/7 pääsynvalvontaa pilveen ja sisäiseen verkkoon. Lokien pitäminen (29 %) kaikista pääsy-yrityksistä (sekä onnistuneista että epäonnistuneista) ja kriittisiksi tunnistettujen tietojen koskemattomuuden seuranta olivat myös yleisimpien keinojen joukossa.

Suurissa yrityksissä ylläpidetään myös lokia pääsy-yrityksistä järjestelmiin (54 %) ja niistä yli puolet (56 %) ylläpitää jatkuvaa 24/7 pääsynvalvontaa pilveen ja sisäiseen verkkoon.

Pienet vastaajayritykset eroavat muista arkaluontoisten tietojen tallennuksen ja säilyttämisen ulkoistamisessa. Niistä kolmasosa (30 %) tekee näin, kun suurilla (6 %) ja keskisuurilla (12 %) vastaajilla se on harvinaisempaa. Kyse on oletettavasti resursseista. Pilvipalveluissa on etunsa, mutta myös riskinsä. Pilveen tallentavan on tärkeä tarkastaa sopimuksissa luvattu turvallisuuden taso. Pienillä toimijoilla valitettavasti ei yleensä ole osaamista ja aikaa tehdä auditointeja, mutta yrityksen arkaluontoinen tieto tulisi suojata tehokkaasti myös pilvipalvelussa.

Miten rajoitatte pääsyn tärkeisiin ja/tai luottamuksellisiin yritystietoihin?

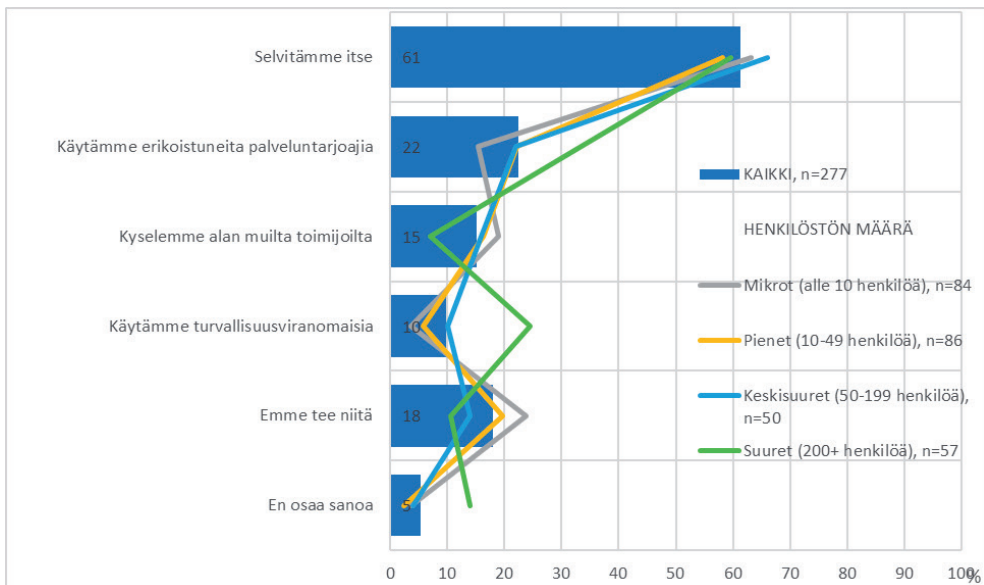


Ulkomaisten liikekumppanien ja heidän yhteyksiensä taustatutkimukset

Ulkomaisten liikekumppaneiden (yritysten ja/tai yksityishenkilöiden) ja heidän yhteyksiensä taustatutkimukset tehdään useimmiten itse (61 %) tai niihin käytetään erikoistuneita palveluntarjoajia (22 %). Kolmasosa suurista yrityksistä käyttää turvallisuusviranomaisia (34 %) tai erikoistuneita palveluntarjoajia (30 %).

Vaikuttamisen ja vakoilun riskin pienentämisen lisäksi taustantarkastukset ovat tarpeen lahjonnanvastaisen toiminnan, kansainvälisten pakotteiden rikkomisen, rahanpesun ja terrorismin rahoittamisen estämiseksi. Kansainvälisesti toimivan yrityksen on siis hyvä selvittää liikekumppaniensa taustat jo monen muun syyn kuin hybridivaikuttamisen vuoksi. Samoilla markkinoilla tai kohdemaassa toimivat keskenään kilpailemattomat yritykset voisivat tehostaa toimintaa tekemällä yhteistyötä turvallisuuteen liittyvässä toiminnassa.

Miten teette kotimaisten ja ulkomaisten liikekumppanien (yritysten ja/tai yksityishenkilöiden) ja heidän yhteyksiensä taustatutkimukset?



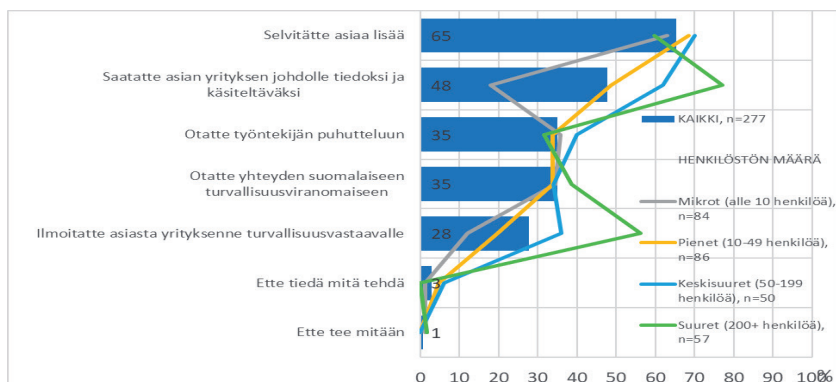
Toiminta epäiltäessä työntekijän sekaantuneen johonkin laittomaan tai yritykselle haitalliseen toimintaan

Tällä kysymyksellä selvitettiin yritysten reagointia epäilyksen tullessa sen tietoon. Erilaisiin väärinkäytöksiin liittyy usein se tosiasia, että epäilyttävästä toiminnasta on ollut tietoa yrityksen muilla työntekijöillä, mutta asiaan ei ole puututtu tai työntekijät eivät ole tienneet kenelle asiasta ilmoittaa. Siksi yritysten olisi hyvä ottaa käyttöön esimerkiksi väärinkäytösten ilmoituskanava, jolla voi alentaa erilaisten epäiltyjen väärinkäytösten ilmoituskynnystä ja samalla tarjota työntekijöille helpon tavan tukea yrityksen turvallisuustyötä.

Yleisin reagointitapa vastaajayritysten keskuudessa (66 %) oli käynnistää lisäselvitys epäilyksen tiimoilta. Toiseksi yleisin reagointitapa oli saattaa asia johdon tietoon ja käsiteltäväksi (48 %). Näissä tavoissa on hyvää se, ettei työnantaja suinpäin ryhdy suoraan toimintaan työntekijän suhteen. Tällainen selvittely voi tuoda esille seikkoja, joiden seurauksena on hyvä ottaa yhteyttä viranomaisiin. Tiedot voivat olla sellaisia, ettei niitä enää ole saatavilla sen jälkeen, kun työntekijään on otettu yhteyttä.

Kolmasosa kaikista vastaajayrityksistä (35%) ottaisi työntekijän puhutteluun tai ottaisi yhteyttä turvallisuusviranomaiseen. Ennen näitä toimenpiteitä työnantajan kannalta olisi hyvä selvittää mahdollisimman paljon tosiasioita asian tiimoilta. Hieman alle kolmasosa (28 %) ilmoittaisi asian yrityksen turvallisuusvastuutaavalle.

Mitä teette, jos epäilette, että jokin tietoonne tullut työntekijäanne kohdistuva tai häneen liittyvä toiminta voisi olla jotain laitonta tai yrityksellenne haitallista?



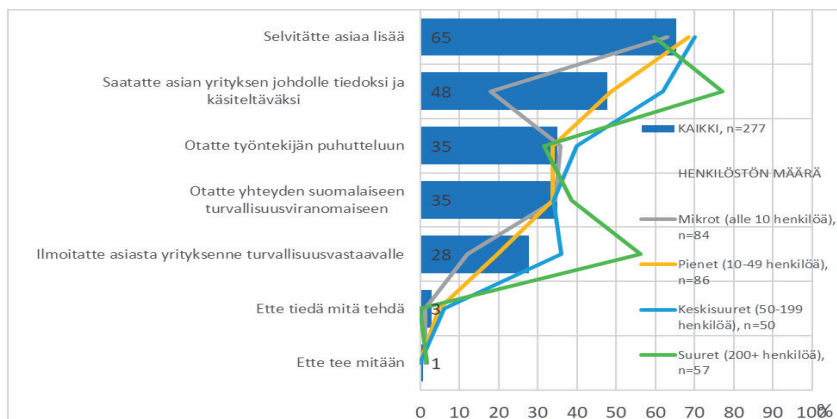
Tiedonsaantikanavat hybridivaikuttamiseen liittyvästä toiminnasta ja toimijoista

Tällä kysymyksellä selvitettiin yritysten reagointia epäilyksen tullessa sen tietoon. Erilaisiin väärinkäytöksiin liittyy usein se tosiasia, että epäilyttävästä toiminnasta on ollut tietoa yrityksen muilla työntekijöillä, mutta asiaan ei ole puututtu tai työntekijät eivät ole tienneet kenelle asiasta ilmoittaa. Siksi yritysten olisi hyvä ottaa käyttöön esimerkiksi väärinkäytösten ilmoituskanava, jolla voi alentaa erilaisten epäiltyjen väärinkäytösten ilmoituskynnystä ja samalla tarjota työntekijöille helpon tavan tukea yrityksen turvallisuustyötä.

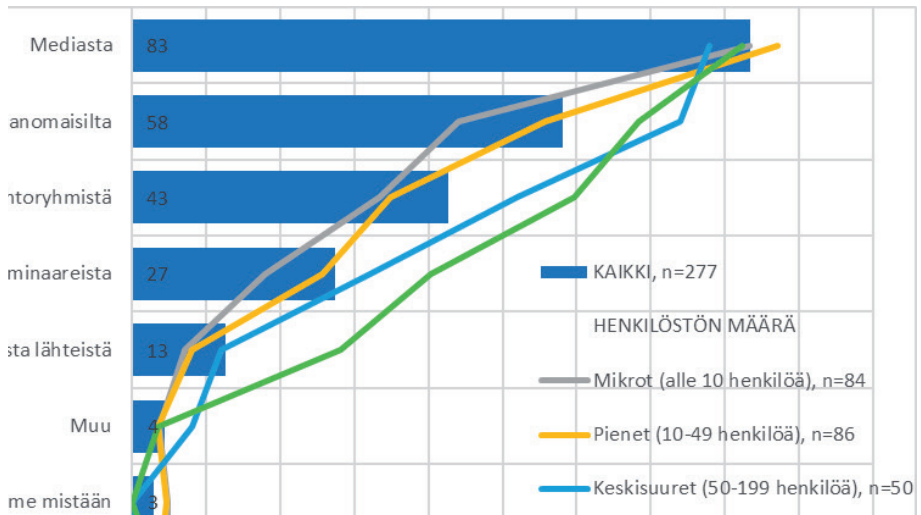
Yleisin reagointitapa vastaajayritysten keskuudessa (66 %) oli käynnistää lisäselvitys epäilyksen tiimoilta. Toiseksi yleisin reagointitapa oli saattaa asia johdon tietoon ja käsiteltäväksi (48 %). Näissä tavoissa on hyvää se, ettei työnantaja suinpäin ryhdy suoraan toimintaan työntekijän suhteen. Tällainen selvittely voi tuoda esille seikkoja, joiden seurauksena on hyvä ottaa yhteyttä viranomaisiin. Tiedot voivat olla sellaisia, ettei niitä enää ole saatavilla sen jälkeen, kun työntekijään on otettu yhteyttä.

Kolmasosa kaikista vastaajayrityksistä (35%) ottaisi työntekijän puhutteluun tai ottaisi yhteyttä turvallisuusviranomaiseen. Ennen näitä toimenpiteitä työnantajan kannalta olisi hyvä selvittää mahdollisimman paljon tosiasioita asian tiimoilta. Hieman alle kolmasosa (28 %) ilmoittaisi asian yrityksen turvallisuusvastaavalle.

Mitä teette, jos epäilette, että jokin tietoonne tullut työntekijäanne kohdistuva tai häneen liittyvä toiminta voisi olla jotain laitonta tai yrityksellenne haitallista?



Tiedonsaantikanavat hybridivaikuttamiseen liittyvästä toiminnasta/toimijoista

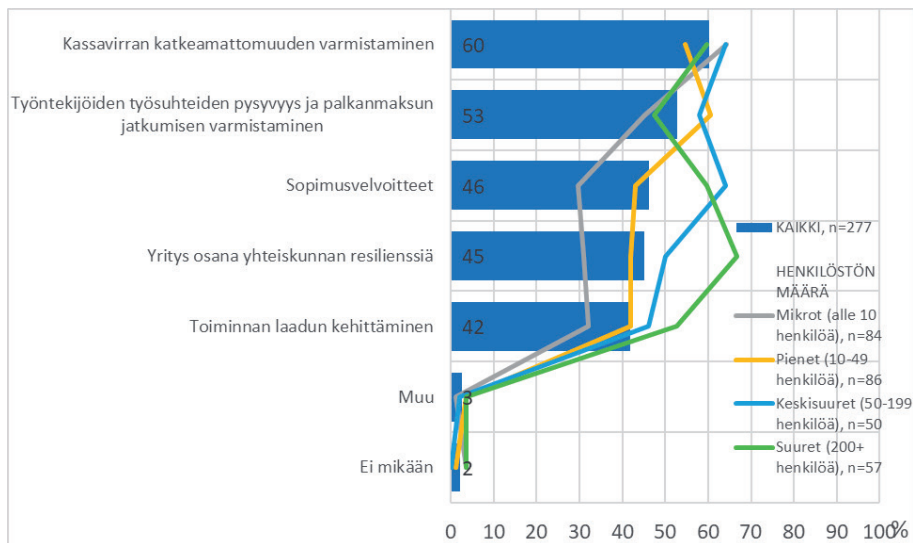


Mikä saa yritykset kehittämään yrityksen kestävyyttä ja jatkuvuussuunnittelua?

Lähes kaksi kolmasosaa vastaajayrityksistä (60 %) kehittäisi kestävyytään ja jatkuvuutta varmistaakseen kassavirran katkeamattomuuden. Yli puolet (51 %) tekee niin varmistaakseen työsuhteiden pysyvyyden ja palkanmaksun jatkumisen. Seuraavaksi yleisimpinä motiiveina ovat sopimusvelvoitteet (46 %), yrityksen rooli osana yhteiskunnan resilienssiä (45 %) ja toiminnan laadun kehittäminen (42 %).

Yritysten motivoiminen jatkuvuuden kehittämiseen on tällä hetkellä ajankohtainen aihe. Monella yrityksellä on sopimusperusteinen velvoite huolehtia jatkuvuudestaan asiakkuuksiansa vuoksi. Sopimussuhde on viime kädessä suoraan yhteydessä kassavirtaan, työsuhteiden pysyvyyteen ja palkanmaksuun. Tulosten myötä on selvää millä kulmalla yrityksiä on lähestyttävä, jotta ne saadaan motivoitumaan jatkuvuuden kehittämiseen.

Mikä saa tai saisi teidät kehittämään yrityksenne kestävyyttä ja jatkuvuussuunnittelua?



Yritysten kyky tunnistaa informaatiovaikutusta

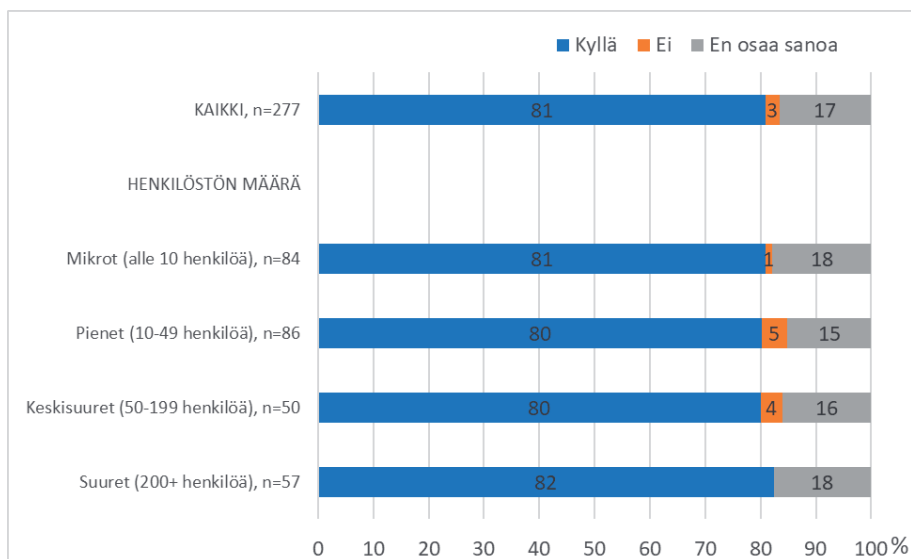
Valtaosa yrityksistä (81 %) vastaa tunnistavansa informaatiovaikuttamisen. Valeuutiset, disinformaatio ja muut tavat vaikuttaa ihmisten ajatteluun ja mielipiteisiin ovat kustannuksiltaan halpoja ja demokratoita vastaan suunnattuina tehokkaita.

Hybridivaikuttamisen keinot ovat tuoneet valtioiden välisen rintaman tavallisten ihmisten olohuoneisiin. Informaatiovaikuttaminen valeuutisineen kohdistetaan suoraan kansalaisiin ja heidän mielipiteisiin. Mielipidevaikuttamista on aina ollut, mutta digitalisaatio on antanut sille asean joka merkittävästi tehokkaampi kuin mikään informaatiovaikuttamisen väline ennen.

Suuri osa länsimaisen demokratian kansalaisista kantaa kädessään älypuhelinia. Älypuhelimesta voidaan lukea uutisia ja mielipiteitä ympäri vuorokauden. Älypuhelimien ja digitalisaation synnyttämä tehokas alusta on nostanut informaatiovaikuttamisen tehokkuutta siitä mikä se oli vuosikymmen sitten. Yksi hyvin muotoiltu väite voi tavoittaa minuuteissa enemmän ihmisiä kuin television ja paperisanomalehtien valtakautena tavoitettiin viikkojen kuluessa.

Suomalaisten yritysten kykyä tunnistaa informaatiovaikutusta auttaa korkea koulutustaso ja asiasta varsinkin viimeaikoina julkisuudessa käyty keskustelu. Monet ihmiset saavat tietonsa median välittämänä ja kotimaisella medialla on merkittävä rooli informaatiovaikuttamisen vastaisessa toiminnassa. Uutistoiminta ja tiedonjakkaminen informaatiovaikuttamisesta ovat osaltaan auttaneet suomalaisia kehittymään ilmiön tunnistamisessa ja sen kohtaamisessa.

Osaatteko tunnistaa informaatiovaikuttamista? (Kuten valeuutiset, disinformaatio, oikean tiedon irrottaminen asiayhteydestä...)



”Jos työntekijä huomaa jotakin epäilyttävää, niin siitä on raportoitava yrityksen johdolle välittömästi. Yrityksen johto jatkaa siitä eteenpäin. Johto tekee tarvittavat toimet ja ilmoitukset tapahtuneesta.”

”Kauppakamarit, kehitysyhtiöt, uutiskirjeet”

”Säännöt, ohjeet ja kanavan siihen, miten ilmoitetaan mahdollisesta tunkeutumisesta.”

”Esimerkiksi sisäisten sähköpostien ja niissä olevien linkkien varmistus puhelimitse.”

”Olemme harjoitelleet tunnistamaan kalasteluyrityksiä”

”Ilmoituskynnyksen madaltaminen, tietojen hajauttaminen, epäilyttävien toimeksiantojen sandboxaaminen”.

”Ohjeet tietokoneiden, puhelimien, internetin, sähköpostien käyttämiseen ja verkossa toimimiseen”

”Vieraiden USB yms. laitteiden sekä avoimien verkkojen välttäminen.”

”Sovittu ketkä vastaavat uusilta tahoilta tuleviin kyselyihin. Päivitetty ja kerrattu tietosuojaohteet.”

”Käyttäjille suunnattuja ohjeita kuinka toimia erilaisissa tilanteissa sekä yleistä informointia.”

”Ilmoituskanava havaintoja varten.”

”Ohjeistus miten toimia jos epäilyttäviä kontakteja lähestyy.”

”Taustaselvitykset, riskianalyysit, ilmoituskanavat ja koulutus.”

RIKOLLISUUDEN JA HYBRIDIVAIKUTTAMISEN SEURAUKSET

Yrityksille koituvat seuraukset rikollisuudesta voivat yrityksen osalta olla osin samoja kuin hybridivaikuttamisen kohteeksi joutuessaan tai sen jälkeen. Rikolliset voivat hakea vastaavia tietoja kuin vaikuttamisoperaatiossa voidaan hakea ja hyödyntää. Varautuminen rikoksiin antaa samalla suojaa hybridivaikuttamisen suhteen. Toisaalta hybridivaikuttamisoperaatiolla ja siinä mahdollisesti käytettävällä rikollisuudella voi olla samanaikaisia toisistaan eroavia seurauksia sekä yrityksille että kohdemaalle.

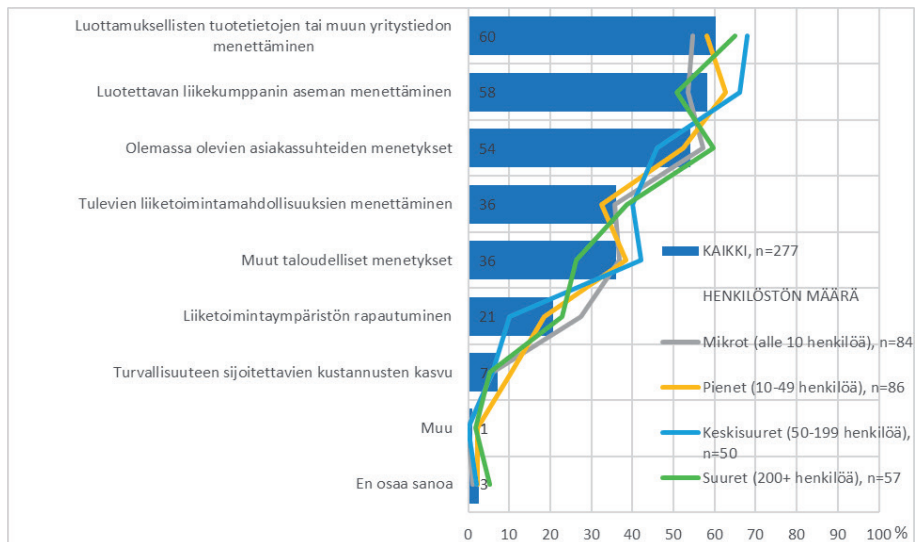
Vakavimmat rikollisuuden aiheuttamat seuraukset yrityksille

Kolme vakavinta rikollisuuden aiheuttamaa seurausta liike-elämälle ovat luottamuksellisten tuotetietojen tai muun yritystiedon menettäminen (60 %), luotettavan liikeyhteistyön aseman menettäminen (58 %) ja nykyisten asiakassuhteiden menetykset (54 %).

Kolmasosan (36 %) mielestä muut taloudelliset menetykset ovat yksi vakavista rikollisuuden aiheuttamista seurauksista.

Yritykset tiedostavat luottamuksellisten tietojen merkityksen yritystoiminnalle. Näille tiedoille on käyttöä rikollisin keinoin toimiville kilpailijoille. Maineen menettäminen ja asiakasmenetykset vaikuttavat yrityksen kilpailuasemaan ja kassavirtaan aivan kuten luottamuksellisten tietojen menettäminen.

Mitkä ovat kolme vakavinta rikollisuuden aiheuttamaa seurausta yrityksille?



Vakavimmat seuraukset hybridivaikuttamisesta

Kolme vakavinta seurausta hybridivaikuttamisesta ovat kansallisen itsenäisyyden tai päättäväisyyden rapauttaminen (53 %), luottamuksellisten tietojen (yritys tai valtio) menettäminen (52 %) ja vaikutus poliittiseen päätöksentekoon (51 %).

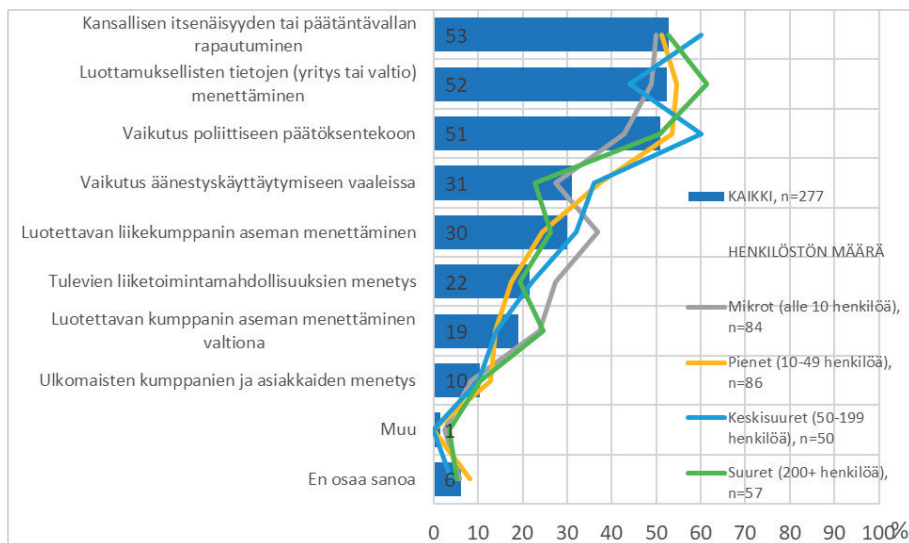
Hybridivaikuttamisen tavoitteena voi olla erilaisia asioita. Jotain yhteiskunnallista kehityskulkua voidaan pyrkiä hidastamaan, estämään tai vastavuoroisesti asiantila pyritään pitämään ennallaan ja toimet valikoituvat sen mukaan. Osa toiminnasta peittyä normaalin yhteiskunnallisen toiminnan kaltaiseksi. Mieli-
devaikuttaja voi tehdä työtään omasta ideologiastaan lähtien tai sitten vieraan vallan tavoitteita tukien. Kuulijan tai lukijan silmissä mielipiteet saattavat vaikuttaa vain poliittiselta kannanotolta.

Kybertoiminnalla voidaan varastaa tietoa, estää palveluja tai valmistella ja toteuttaa sabotaaseja. Informaatiovaikuttamisella pyritään yleensä vaikuttamaan kansan mielipiteeseen ja ehkä valtiojohtoon toimintaan jonkin asian suhteen. Fyysisellä vaikuttamisella voidaan vaikuttaa yksilöihin lahjomalla, painostamalla,

houkuttelemalla tai muilla vastaavilla tavoilla. Näissä käytettävää tietoa on taas saatu kybervakoilun tai perinteisemmän vakoilun keinoin tai tiedonantajilta.

Vaikuttamisen lopputulokseen johtanut toiminta ei ulkopuolisin silmin selvästi eroa millään tavalla yhteiskunnan tai yrityselämän normaalista toiminnasta. Lopputuloskin voi vaikuttaa luonnolliselta seuraukselta suhteessa asian kehityskulkuun. Tässä piilee vaikuttamisen ja hybridivaikuttamisen tehokkuus demokraattisessa avoimessa yhteiskunnassa. Mielenpitemvapaus, sananvapaus, vapaa yrityselämä ja avoin yhteiskunta ovat kaikki länsimaisten demokratioiden arvoja, joita vieras valtio voi hyödyntää pyrkiessään vaikuttamaan kohdemaahan.

Mitkä ovat kolme vakavinta seurausta hybridivaikuttamisesta?



Onko havainnut omaan liiketoimintaan tai jonkun muun liiketoimintaan kohdistunutta toimintaa, joka voisi olla hybridivaikuttamista tai sen osa?

Yrityksen voi olla vaikea tunnistaa hybridivaikuttamista tai vaikuttamista toiminnan alkuvaiheessa. Yritykseen voi kohdistua jonkinlaista vaikuttamista, mutta sen kytkeminen varmuudella osaksi suurempaa useamman keinon kokonaisuutta on usein yrityksen mahdollisuuksien ulkopuolella. Olennaista on, että yritys tunnis-

taisi käynnissä olevan jotain normaalista poikkeavaa ja sen suhde viranomaisiin olisi toimiva ja se osaisi antaa tiedon viranomaiselle. Viranomaisen rooli on yhdistää tietoja ja arvioida onko kyseessä yksittäistapaus vai osa useamman keinon hybridioperaatiota ja mitä toiminnalla tavoitellaan. Ja sitten muodostaa päätös siitä miten eri viranomaiset asiaan reagoivat.

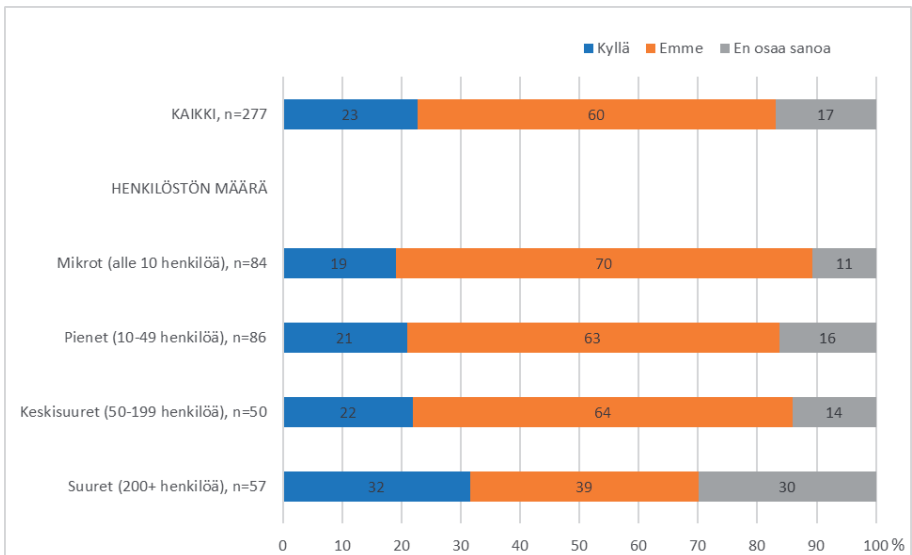
Viidesosa (17 %) kaikista vastaajista ei osaa sanoa ovatko ne kohdanneet epäiltyä hybridi vaikuttamista. Kolmasosa (30 %) suurista yrityksistä ei myöskään osannut sanoa asiasta. Viranomaisten on hyvä ottaa elinkeinoelämään kohdistuva tai sitä hyväksikäyttävä hybridi vaikuttaminen huomioon tulevaisuudessa suunnitelmissaan. Hybridi vaikuttamisella pyritään vaikuttamaan valtion toimintaan ja siksi vetovastuu sen torjunnassa on viranomaisilla. Tehokkain tapa lisätä yritysten osaamistasoa on järjestää koulutuksia ja jakaa tietoa hybridiuhista.

Kaikista vastaajista lähes joka neljäs (23 %) on havainnut omaan liiketoimintaan ja jonkun muun liiketoimintaan kohdistunutta toimintaa, joka voisi olla hybridi vaikuttamista tai sen osa. Tietoisuus vaikuttamisesta ja sen eri ilmenemismuodoista on lisääntynyt vuosien kuluessa.

Kolmasosa suurista yrityksistä (32 %) on havainnut tällaista toimintaa. Suuret yritykset ovat asiakaskuntansa, kontaktiensa ja asemansa vuoksi useammin kohteina hybridi vaikuttamiselle. Vuoden 2018 selvityksestä suuriin yrityksiin kohdistunut epäilty hybridi vaikuttaminen on lisääntynyt 12 prosenttiyksikköä (20 % → 32 %). Kaikkien vastaajien osalla kasvua on ollut 13 prosenttiyksikköä (10 % → 23 %).

Kysyttäessä mistä epäilty toiminta oli kotoisin, vastaus useimmiten on Venäjä tai Kiina. Myös Pohjois-Korea ja Iran mainittiin epäiltyinä toimijoina.

Oletteko havainneet omaan liiketoimintaan tai jonkun muun liiketoimintaan kohdistunutta toimintaa, joka voisi olla hybridivaikuttamista (taustalla rikolliset, toinen yritys, jonkin valtion toimijat tai muu taho)?



”Aiemmassa työssä palvelunestohyökkäyksiä, oletettua lahjontaa tavoitteisiin pääsemiseksi, valeinformaatiota, painostusta. Nykyisessä työssä painostusta, informaatiovaikuttamista.”

”Erilaisia linkkejä asiakkaalta, jota ei ole meille olemassa. Tilauspohjia latauslinkkinä.”

”Sosiaalisen median eri alustoilla

- a) ristiriitaisten agendojen ajaminen/provosointi tilannekuvan sotkemiseksi**
- b) aktiivinen ”mustavalkoistaminen”/kärjistäminen omien etujen ajamiseksi tilannetta (Ukraina) hyväksikäyttäen.”**

”Verkkokaupan ja kassan toimintahäiriöt, kohdistuu siis toissijaisesti meihin, koska ostetaan ulkopuoliselta palveluntarjoajalta.”

”Epämääräiset liikemieheksi itseään tituleeranneet henkilöt kutsuivat paikallisia yrityksiä yritysten välisen yhteistyön kehittämismatkalle Kiinaan paikallisen kunnallisen yritystukiorganisaation tuella.”

”Pankin kautta välitettävän maksuliikenteen häirintä/hakkerointi/ palvelunesto maksuerässä, jossa menee mm. ajallaan maksetut arvonlisäverot ja ennakonpidätykset.”

”It-infraan kohdistuneet palvelunestot ja sabotaasit”

”Epämääräisten kontaktipyyntöjen määrän kasvu esimerkiksi LinkedIn verkostossa.”

”Entinen tiedustelu-upseeri haki avoinna ollutta työpaikkaa toimistossamme.”

”Olemme toistuvien tiedonkalasteluyritysten kohteena. Osa viesteistä on täysin uniikkeja meihin kohdistettuja, osa ”normaalia” Internetissä tapahtuvaa kalastelua. Yrityksen johtotason henkilöstöä on myös henkilökohtaisesti lähestytty.”

”Viime aikoina meille on pyrkinyt ilmaiseen harjoitteluun ja/ tai hakenut töihin henkilöitä, joiden on epäilty pyrkineen töihin hankkiakseen tietoa asiakkaitamme. Esimerkiksi maisteri-tason opinnot Venäjällä suorittanut henkilö huomattavalla työkokemuksella, joka ei tosin pitänyt kokonaan paikkaansa, oli hakemassa ilmaiseen harjoitteluun, vaikka ko. CV:llä olisi päässyt haastatteluun avoimena olevaan työtehtävään.”

”Luottamuksen menettäminen valtiona ja ulkomaisten investointien väheneminen, kansainvälisen liiketoiminnan ja muun aktiivisen vuorovaikutuksen väheneminen. Talouden kurjistuminen. Oikeusvaltion statuksen menettäminen.”

”Anastettujen yhteystietojen käyttö yrityksemme nimissä hybridivaikutukseen pyrkimisessä.”

YRITYSTEN ODOTUKSET VIRANOMAISILTA JA YHTEISTYÖ

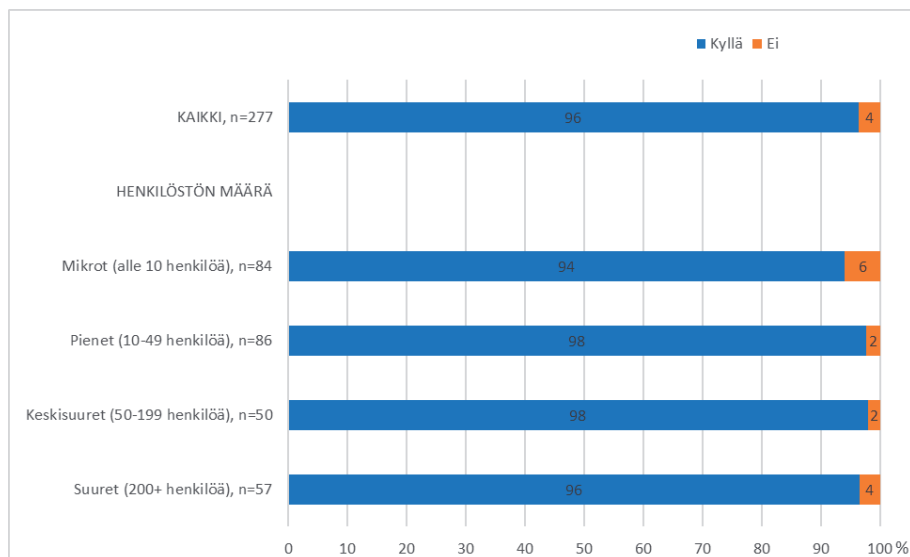
Yritysturvallisuuden parissa on Suomessa hyvä viranomaisten ja yritysten välinen yhteistyö. Usein on todettu ettei vastaavanlaista toimivaa mallia ole muualla. Kaikessa yhteistyössä on muistettava kyseessä olevan molempia tahoja palvelevan toiminnan. Kauppakamarien selvityksissä seitsemäntoista vuoden aikana on käynyt selväksi, että yritykset yleensä kaipaavat viranomaisilta tietoa, koulutusta ja neuvoja.

Koulutus ja tieto ovat tehokkain tapa nostaa yritysten osaamistasoa. Lisäksi tarvitaan toimivaa tiedonvaihtoa yritysten ja viranomaisten välillä. Yritykset toimivat kaikkialla Suomessa ja koulutuksen sekä tiedon myötä ne voivat tunnistaa epäilyä toimintaa ja antaa tietoa siitä tiedonvaihtofoorumille tai viranomaisille. Yhteiskuntamme on verkottunut monella osa-alueella, mutta hybridi vaikuttamisen torjunnan osalta on yhä tehtävää ja paljon saavutettavaa.

Pitääkö suomalaisten viranomaisten tukea lii- ke-elämää tekemällä oppaita hybridiuhista ja jär- jestämällä koulutuksia ja harjoituksia?

Lähes kaikki vastaajayritykset (96 %) ovat sitä mieltä, että suomalaisten viranomaisten tulee tukea yrityksiä tekemällä oppaita hybridiuhista ja järjestämällä koulutuksia ja harjoituksia. Yritysten tarve tiedolle ja koulutukselle ei jää epäselväksi. Tarve on kasvanut 19 prosenttiyksiköllä neljässä vuodessa (77 % → 96 %).

Pitääkö suomalaisten viranomaisten tukea liike-elämää esimerkiksi tekemällä oppaita hybridiuhista ja järjestämällä koulutuksia ja harjoituksia?

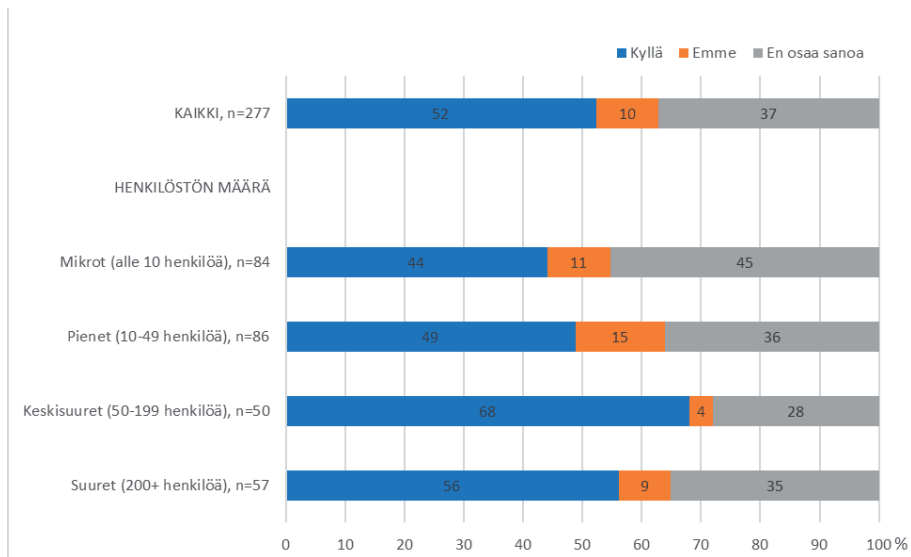


Jakaako yritys tietoa suomalaisille turvallisuusviranomaisille, kun havaitsee yritykseen kohdistuvia epäilyttäviä toimia, joko ulkomailla tai täällä Suomessa?

Puolet vastaajayrityksistä (52 %) jakaa tietoa suomalaisille turvallisuusviranomaisille havaitessaan yritykseen kohdistuvia epäilyttäviä toimia ulkomailla tai Suomessa. Vain kymmenen prosenttia vastaajista ei jaa tällaista tietoa viranomaisille. Suurista yrityksistä yli puolet (56 %) jakaa tietoa.

Yritykset ovat merkittävässä määrin valmiita tekemään yhteistyötä viranomaisten kanssa. Tiedon avulla viranomainen voi ylläpitää tilannekuvaa ja analysoimalla tietoja se voi kyetä luomaan käsityksen siitä millaista toimintaa yrityksiin kohdistuu. Yhteistyön tehostaminen yritysten kanssa vahvistaisi koko yhteiskunnan varautumista hybridivaikuttamiseen. Yhteistyöllä on myös ennaltaehkäisevää vaikutusta.

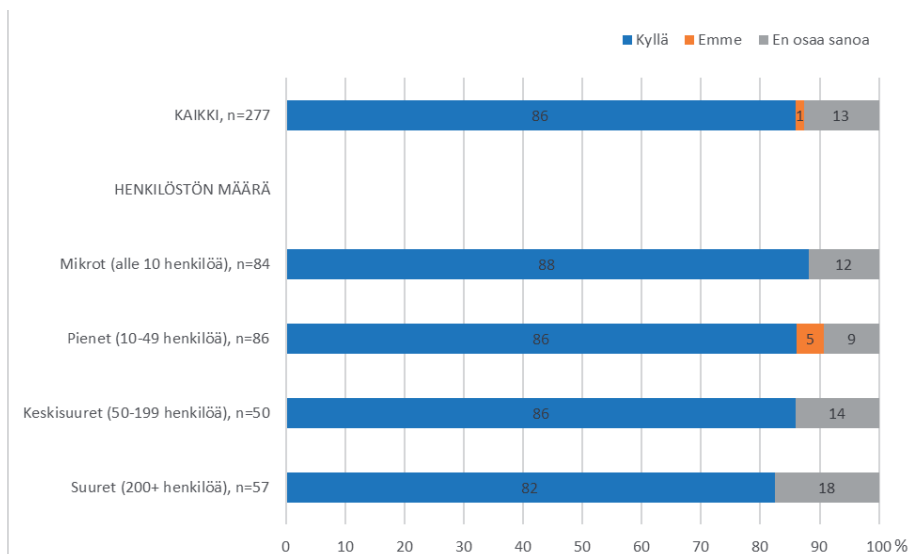
Jaatteko omatoimisesti tietoa suomalaisille turvallisuusviranomaisille, kun havaitsette yritykseenne kohdistuvia epäilyttäviä toimia, joko ulkomailla tai täällä Suomessa?



Jakaisiko yritys tietoa epäilemästään hybridivai- kuttamisesta, jos käytössä olisi suljettu yritysten tai oman alan yritysten suljettu tiedonvaihtoofo- rumi?

Valtaosa vastaajayrityksistä (86 %) jakaisi tietoa suljetulla tiedonvaihtoorumilla. Tiedonvaihto erilaisista epäilyistä on nopea tapa lisätä myös muiden yritysten tietoisuutta ja valmiutta. Tiedonvaihto voi lisätä muuta yhteistyötä yritysten välillä ja ajan myötä tiedonvaihtoyhteisöistä voi syntyä verkostoja, joissa voidaan auttaa toisia verkoston jäseniä toiminnassa erilaisia uhkia vastaan.

Jakaisitteko tietoa epäilemistänne yritykseenne kohdistuneista hybridi-toimista, jos käytössänne olisi nimenomaisesti tällaisen tiedon jakamiseen tarkoitettu suljettu elinkeinoelämän tai oman alanne tiedonvaihtofoorumi?

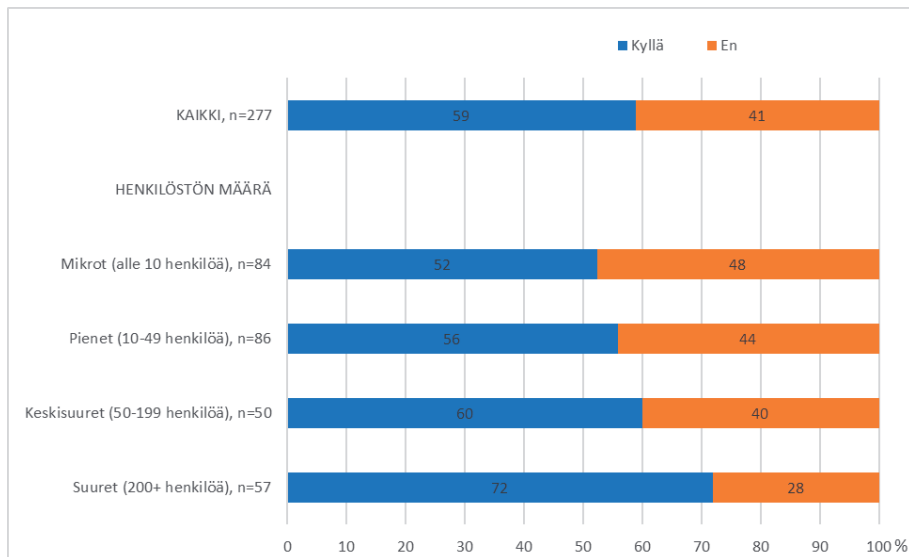


Tietävätkö yritykset miltä suomalaiselta viranomaiselta saa tietoa ja apua epäilemäänsä hybridivaikuttamiseen liittyen

Yli puolet vastaajayrityksistä (59 %) tietää miltä viranomaiselta saa tietoa ja apua epäillessään hybridivaikuttamista. Yleisimmin oikea vastuuviranomainen tunnetaan suurten vastaajien (72 %) keskuudessa. Kaikista vastaajista 41 prosenttia ei kuitenkaan tiedä vastuuviranomaista.

Viranomaisilla on yhä tehtävää lisätäkseen yritysten tietoisuutta oikeasta viranomaisesta hybridivaikuttamisen suhteen. Mikäli yritys ei tiedä mihin olla yhteydessä, on selvää ettei viranomainen saa kaikkea tarpeellista tietoa toimintansa perustaksi. Viranomaiset tarvitsevat enemmän resursseja yritysten auttamiseen. Viranomaisten tulee hankkia yritystoimintaa tuntevia osaajia, jotka osaavat toimia ja viestiä yritysten kanssa.

Tiedättekö miltä suomalaiselta viranomaiselta saatte tietoa ja apua, jos epäilette yritykseenne kohdistuvan hybridivaikuttamiseen liittyvää toimintaa?

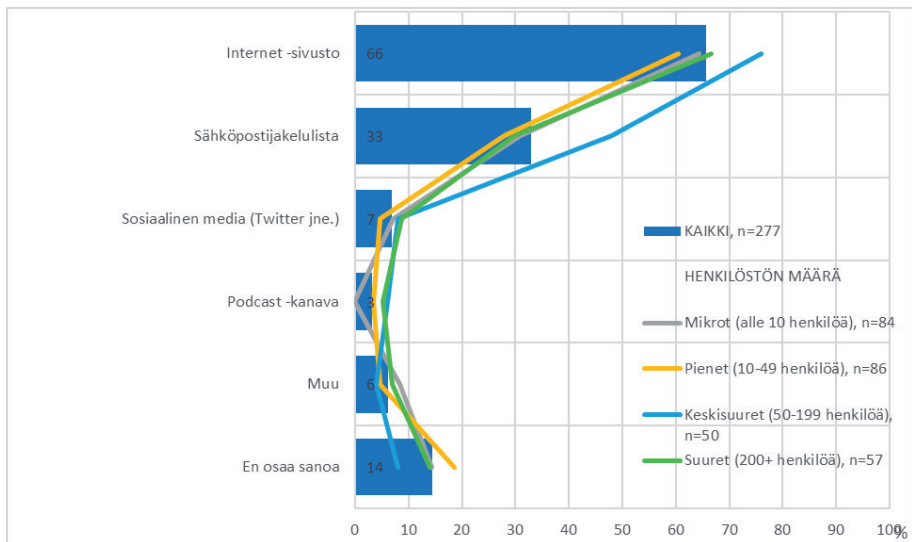


Mikä olisi paras tiedonjakokanava jatkuvuuden kehittämiseen liittyvän tiedon jakamiseen?

Kahden kolmasosan mielestä internetsivusto (66 %) olisi paras tapa jakaa jatkuvuuteen liittyvää tietoa. Sähköpostijakelulista (33 %) sai toiseksi eniten kannatusta. Sosiaalinen media (7 %) oli kolmanneksi suosi-tuin vaihtoehto, mutta jäi kauas internetsivuston kannatuksesta.

Avoimen tiedon jakamisessa internetsivusto on kustannustehokkain tapa. Sivusto on matalan kynnyksen tapa jolla voi helposti herättää yritysten mielenkiintoa kehittää jatkuvuutta ja iskunkestävyyttä.

Jos käytettävissä olisi jatkuvuuden kehittämiseen liittyvä tiedonjakokanava, olisiko paras toteutustapa?



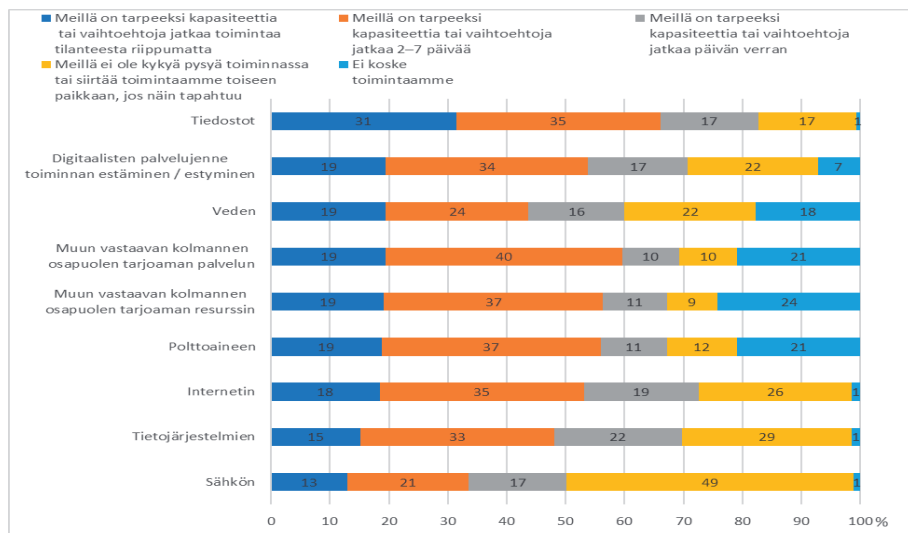
YRITYSTEN KYKY KESTÄÄ ERI RESURSSIEN SAATAVUUDEN HÄIRIÖITÄ

Hybridivaikuttaminen ja jatkuvuus?

Hybridivaikuttaminen voi pahimmillaan estää normaalitilanteessa käytettävissä olevien yhteiskunnan infran resurssien käyttämisen. Tuotannon katkaiseminen ja laajempi liiketoiminnan häiritseminen voivat olla osana ”näkyvän vaiheen” hybridivaikuttamista. Tässä vaiheessa vaikuttamisella on tarkoitus saada aikaan arjessa näkyviä haittoja. Varautuakseen tähän yritys tarvitsee jatkuvuussuunnitelman, jonka avulla se kykenee jatkamaan ainakin osin toimintaansa.

Kyse ei yrityksen kannalta ole pelkästä hybridivaikuttamisen vuoksi tapahtuvasta varautumisesta, vaan kassavirran varmistamisesta arjessa vastaantulevien häiriöiden ja katkosten varalta. Sama varautumistyö auttaa automaattisesti kohdatessa tahallisten tekojen aiheuttamia häiriöitä ja katkoksia. Yrityksen kassavirran varmistamiseksi tekemä varautumistyö on osa yhteiskunnan resilienssiä ja torjuu osaltaan vieraan vallan aiheuttaman iskun seurauksia yhteiskunnalle.

Miten hyvin yrityksenne kestää seuraavien asioiden menetyksen?



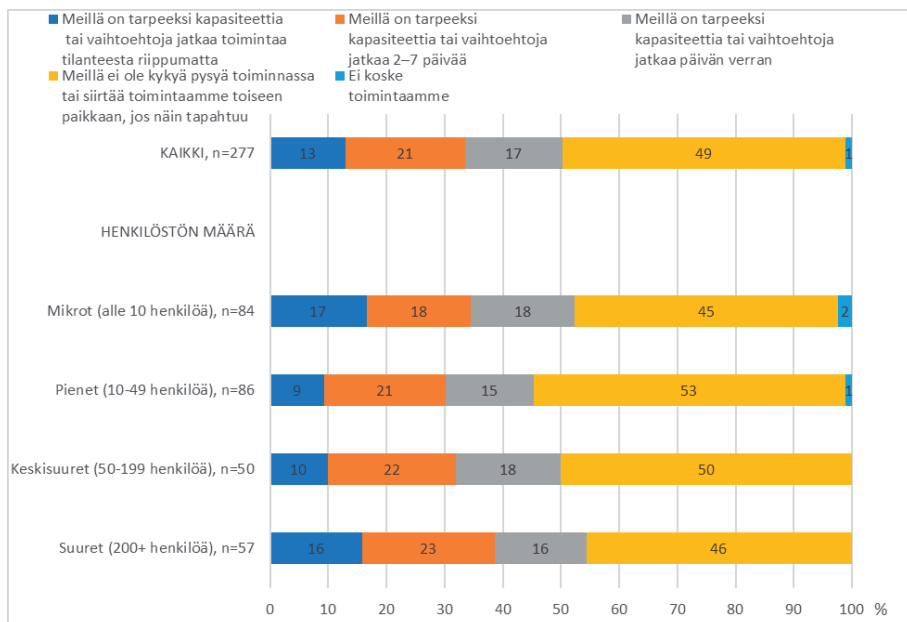
Sähkö

Sähkön menetys vaikuttaa lähes kaikkien yritysten toimintaan. Pidemmän aikaa kestäville sähkökatkoilla on myös laajoja heijastevaikutuksia. Ne voivat haitata esimerkiksi polttoaineen saatavuutta, ruuan valmistamista, päivittäistavaroiden ostamista kaupasta, tietojärjestelmien ja sovellusten käyttöä.

Sähkökatkoksen sattuessa puolet vastaajayrityksistä (49 %) ei kykene pysymään toiminnassa tai siirtämään toimintaa toiseen paikkaan. Yhden päivän sähkökatkoksen kestää noin viidesosa (17 %) vastaajayrityksistä. Tämä tarkoittaa että yhden päivän jälkeen kaksi kolmasosaa (66 %) yrityksistä ei kykene jatkamaan toimintaansa. Suuristakin yrityksistä yli puolet (52 %) on tässä vaiheessa kyvyttömiä jatkamaan toimintaansa. Suurista yrityksistä miltei puolet (46 %) ei kestä sähkökatkoa lainkaan, vaan toiminta keskeytyy sähkönsaannin katkettua.

Kaikista vastaajayrityksistä 41 prosenttia on varautunut suunnittelemaan sitä, miten jatkaa toimintaa sähkönsaannin häiriön sattuessa. Melkein kaksi kolmasosaa (59 %) vastaajayrityksistä ei ole suunnitellut jatkuvuutta sähkön saatavuuden häiriöiden varalta. Sähkökatkoja sattuu ympäri Suomea päivittäin. Ne eivät yleensä ole pitkiä ja siksi monen yrityksen on mahdollista varautua niihin kevyillä toimilla kuten hankkimalla varavirtalähteitä.

Miten hyvin yrityksenne kestää sähkön menetyksen?



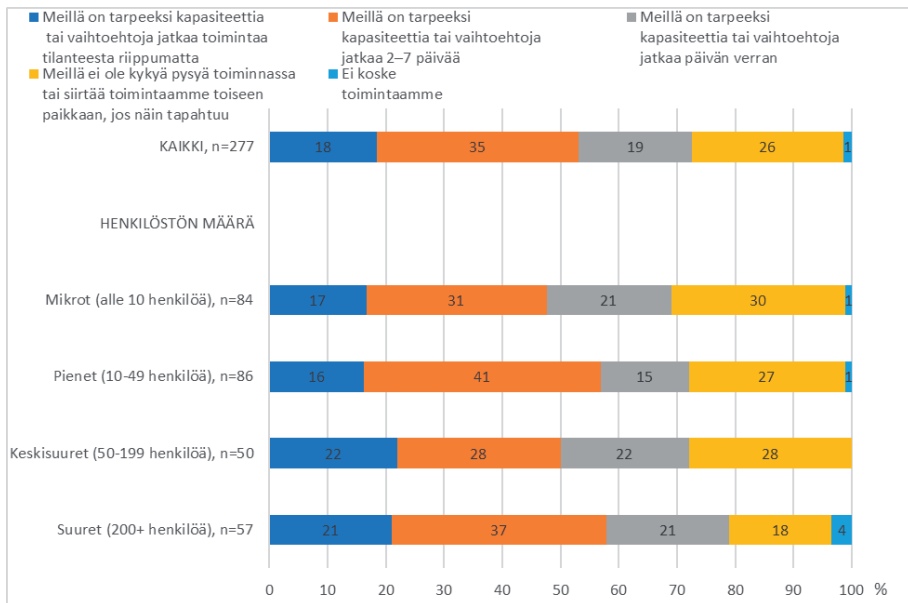
Internet

Noin viidesosa vastaajayrityksistä kestää internetin menetyksen (18 %). Kaikkien yritysten toiminta ei ole kokonaisuudessaan riippuvaista internetin toimivuudesta. Neljäsosa (25 %) vastaajista ei toisaalta selviä hetkeäkään ilman sitä.

Yhden päivän ajan selviää viidesosa (19 %) vastaajayrityksistä. Tämä tarkoittaa että yhden päivän jälkeen melkein puolet (45 %) yrityksistä ei kykene jatkamaan toimintaansa. Suuristakin yrityksistä reilu kolmasosa (39 %) on tässä vaiheessa kyvyttömiä jatkamaan toimintaansa. Viidesosa suurista (21 %) ja keskisuurista (22 %) kestävät internetin menetyksen kokonaan ja kykenevät jatkamaan toimintaansa ilman sitä.

Kaikista vastaajayrityksistä puolet (47 %) on varautunut suunnittelemalla sitä, miten jatkaa toimintaa ilman pääsyä internettiin. Puolet (53 %) vastaajayrityksistä ei siis ole suunnitellut jatkuvuutta internetin katkosten varalta. Syitä näihin katkoksiin voi olla monia, mutta yksinkertaisimmillaan yritys voi varautua käyttämällä useamman kuin yhden teleoperaattorin palveluja. Todennäköisyys useamman teleoperaattorin toiminnan samanaikaiselle estymiselle on hyvin pieni.

Miten hyvin yrityksenne kestää internetin menetyksen?



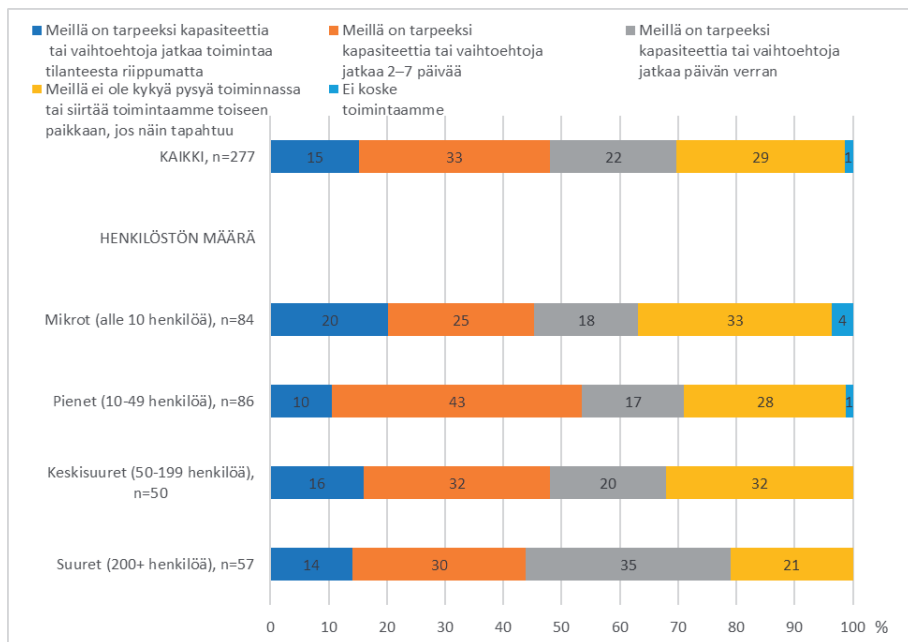
Tietojärjestelmät

Tietojärjestelmien menetyksen kestää 15 prosenttia vastaajista. Noin kolmasosa (29 %) ei pysty toimimaan lainkaan ilman niitä. Tietojärjestelmien käyttö voi estyä teknisistä syistä tai tahallisen teon seurauksena.

Viidesosa (22 %) vastaajayrityksistä kestää yhden päivän ajan. Yhden päivän jälkeen siis puolet (51 %) vastaajayrityksestä ei kykene jatkamaan tietojärjestelmiä. Suuristakin yrityksistä yli puolet (56 %) on tässä vaiheessa kyvyttömiä jatkamaan tietojärjestelmistä riippuvaista toimintaa.

Kaikista vastaajayrityksistä yli puolet (51 %) on varautunut suunnittelemalla sitä, miten jatkaa toimintaa ilman tietojärjestelmiä. Puolet (49 %) vastaajayrityksistä ei siis ole suunnitellut jatkuvuutta tietojärjestelmien käytön estymisen varalta. Harva yritys voi jatkaa toimintaansa ilman tietojärjestelmiä, mutta niiden käytön estymisen ei automaattisesti tarkoita että yrityksen koko toiminta estyy välittömästi.

Miten hyvin yrityksenne kestää tietojärjestelmien menetyksen?



Vesi

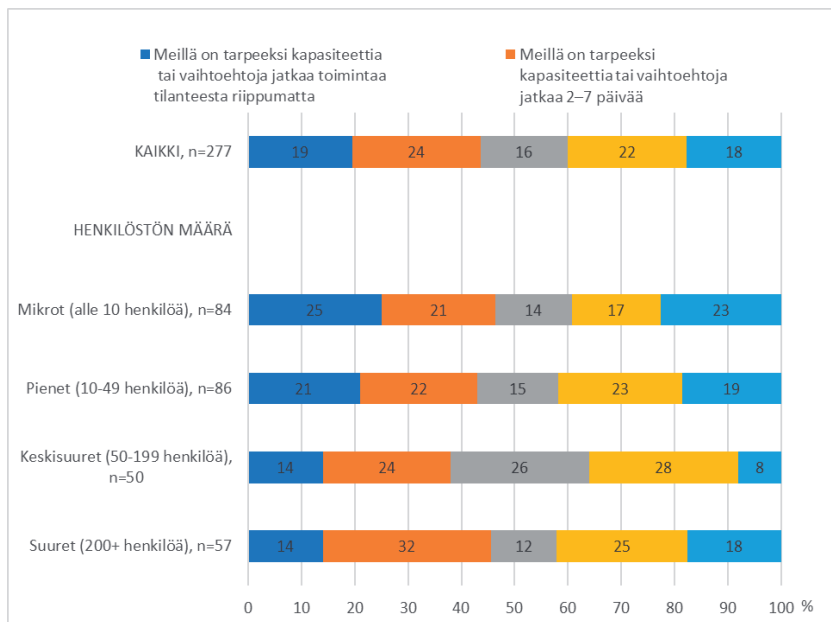
Päivittäinen toiminta on hyvin riippuvaista vedestä. Ihminen menehtyy mikäli vettä ei ole saatavilla kolmeen päivään. Vettä tarvitaan päivittäin ruoanlaitosta alkaen aina teollisuuden tuotantoprosesseihin.

Veden menetyksen kestää viidesosa (19 %) vastaajayrityksistä. Viidesosa (22 %) ei toisaalta kestä ilman vettä päivääkään. Viidesosa (18 %) ilmoitti ettei veden saatavuus koske heidän toimintaansa.

Kuusitoista prosenttia vastaajayrityksistä kestää yhden päivän ajan ilman vettä. Yhden päivän jälkeen yli kolmasosa (38 %) yrityksistä ei kykene jatkamaan toimintaansa. Suurista yrityksistä yli kolmasosa (37 %) ja keskisuurista yli puolet (54 %) on tässä vaiheessa kyvyttömiä jatkamaan toimintaa.

Kaikista vastaajayrityksistä 41 prosenttia on varautunut suunnittelemalla sitä, miten jatkaa toimintaa ilman vettä. Lähes kaksi kolmasosaa (59 %) vastaajayrityksistä ei siis ole suunnitellut jatkuvuutta veden saatavuuden estymisen varalta. Veden saatavuuden keskeytyminen voi vaikuttaa alueellisesti hyvinkin merkittävästi, mutta viranomaisilla on hyvä valmius ja kokemusta vesijakelun tilapäisestä järjestämisestä.

Miten hyvin yrityksenne kestää veden menetyksen?



Polttoaine

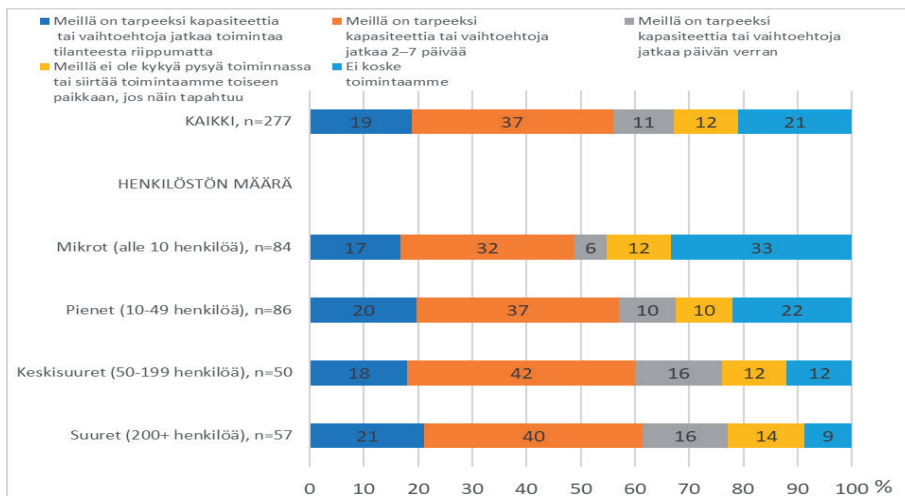
Kaikki yritykset eivät tarvitse yritystoimintaansa polttoainetta, mutta pidempään kestävä polttoaineen saatavuuden loppumisen heijastevaikutukset voivat vaikuttaa merkittävästi yrityksen arkeen. Jos polttoainetta ei ole saatavilla, voivat päivittäistavarakauppojen tavarankuljetukset katketa tai häiriintyä. Tämä voi vaikuttaa päivittäistavaroiden saatavuuteen. Lapset eivät välttämättä pääse kouluun eivätkä vanhemmat työpaikalle.

Viidesosa (19 %) vastaajayrityksistä kestää polttoaineen menetyksen. Tarpeeksi kapasiteettia tai vaihtoehtoja jatkaa toimintaa 2–7 päivää on yli kolmasosalla (37 %) vastaajista. Viidesosa vastaajayrityksistä vastasi ettei polttoaineen saatavuus koske heidän toimintaansa.

Yksitoista prosenttia vastaajayrityksistä kestää yhden päivän ajan. Viidesosa (23 %) yrityksistä ei enää kykene jatkamaan toimintaansa tässä vaiheessa. Suurista yrityksistä melkein kolmasosa (30 %) on päivän jälkeen kyvyttömiä jatkamaan toimintaa.

Kaikista vastaajayrityksistä 41 prosenttia on varautunut suunnittelemalla sitä, miten jatkaa toimintaa ilman polttoainetta. Lähes kaksi kolmasosaa (59 %) vastaajayrityksistä ei siis ole suunnitellut jatkuvuutta polttoaineen saatavuuden loppumisen varalta. Joidenkin yritysten osalta polttoaineen saatavuudella ei kuitenkaan ei ole varautumisen ansiosta vaikutusta toimintaan.

Miten hyvin yritykseenne kestää polttoaineen menetyksen?



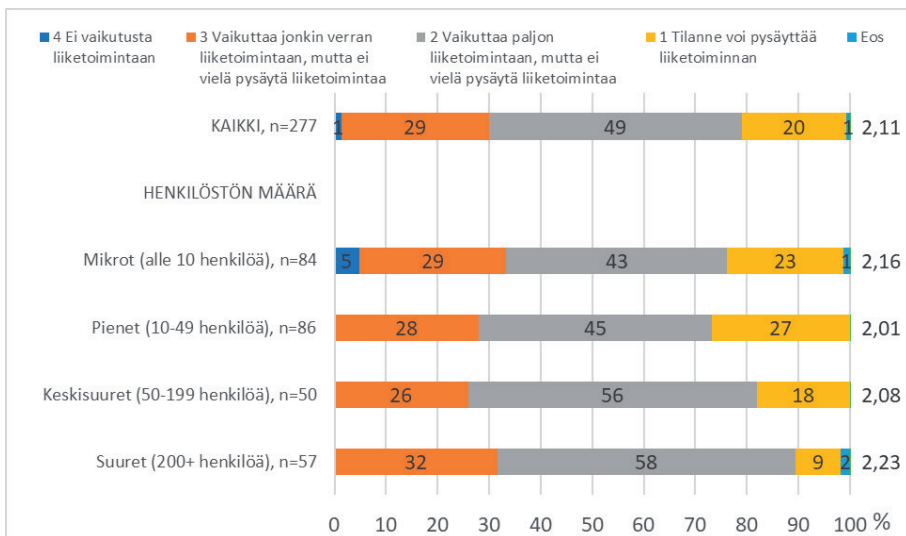
Työvoiman odottamattoman menetyksen (sairastelu) vaikutus yrityksen toimintaan

Korona-aikana yritykset ovat kohdanneet sairauden aiheuttaman vaikutuksen työvoiman saatavuudelle. Yritykset ovat kehittäneet varautumistaan eri keinoin ja niiden kestävyys on aivan toista luokkaa kuin keväällä 2020. Siitä huolimatta laaja sairastelu voi yhä olla haaste yrityksen jatkuvuuden hallinnalle.

Viidesosa (20 %) vastaajayrityksistä ei kestä päivääkään poikkeuksellisen laajaa sairastelua. Puolet yrityksistä (49 %) kestää käytettävissä olevan työvoiman menetyksen vaikka se vaikuttaa paljon yrityksen liiketoimintaan. Hieman alle kolmasosalla (29 %) se vaikuttaa vähintään jonkin verran, mutta se ei pysäytä liiketoimintaa.

Kolmasosalla suurista (32 %) ja neljäsosalla keskisuurista (26 %) menetys vaikuttaa jonkin verran liiketoimintaan. Yli puolella suurista (58 %) ja keskisuurista (56 %) yrityksistä se vaikuttaa paljon liiketoimintaan, mutta ei pysäytä sitä.

Miten hyvin yrityksenne kestää työvoiman odottamattoman menetyksen?



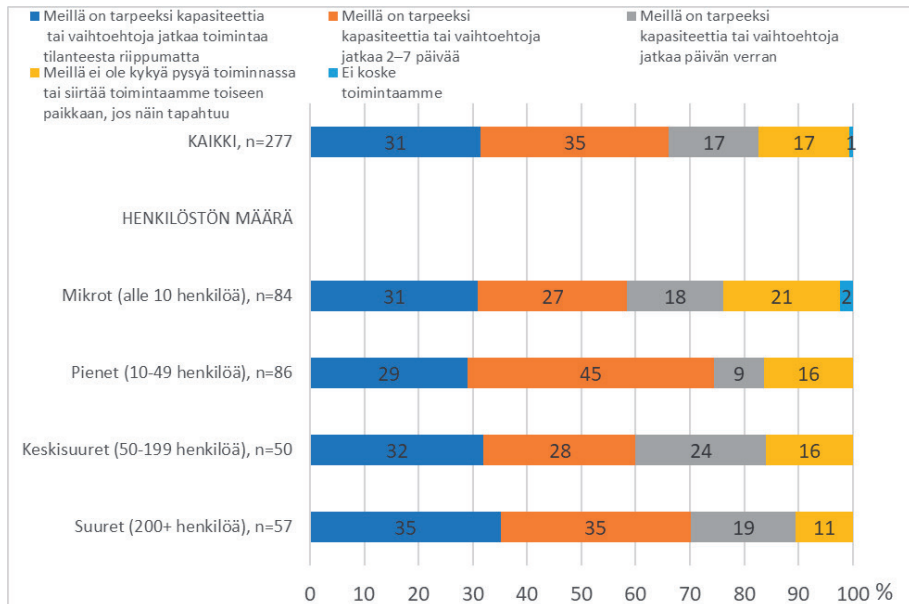
Tiedostojen menetyks

Viidesosa (17 %) vastaajaryityksistä ei pysty jatkamaan toimintaansa päivääkään ilman tiedostoja. Kolmasosa (31 %) yrityksistä kykenee jatkamaan toimintaa ilman tiedostoja. Kolmasosa (35 %) kykenee jatkamaan toimintaa 2-7 päivään. Viidesosa (17 %) selviää päivän verran ilman pääsyä tiedostoihin. Tiedostojen saatavuus ei koske yhtä prosenttia kaikista vastaajista.

Kolmasosa suurista (35 %) ja neljäsosa keskisuurista (28 %) kykenee jatkamaan 2-7 päivään. Kolmasosa suurista (35 %) ja keskisuurista (32 %) kykenee jatkamaan toimintaa ilman tiedostoja.

Kaikista vastaajaryityksistä yli puolet (55 %) on varautunut suunnittelemalla sitä, miten jatkaa toimintaa tiedostojen menetyksen jälkeen. Lähes puolet (45 %) vastaajaryityksistä ei siis ole suunnitellut jatkuvuutta tiedostojen käytön estymisen varalta. Lähes kaikki yritykset tarvitsevat nykyisin tiedostoja toiminnassaan, mutta niiden menettäminen ei välittömästi keskeytä yrityksen koko toimintaa.

Miten hyvin yrityksenne kestää tiedostojen menetyksen?



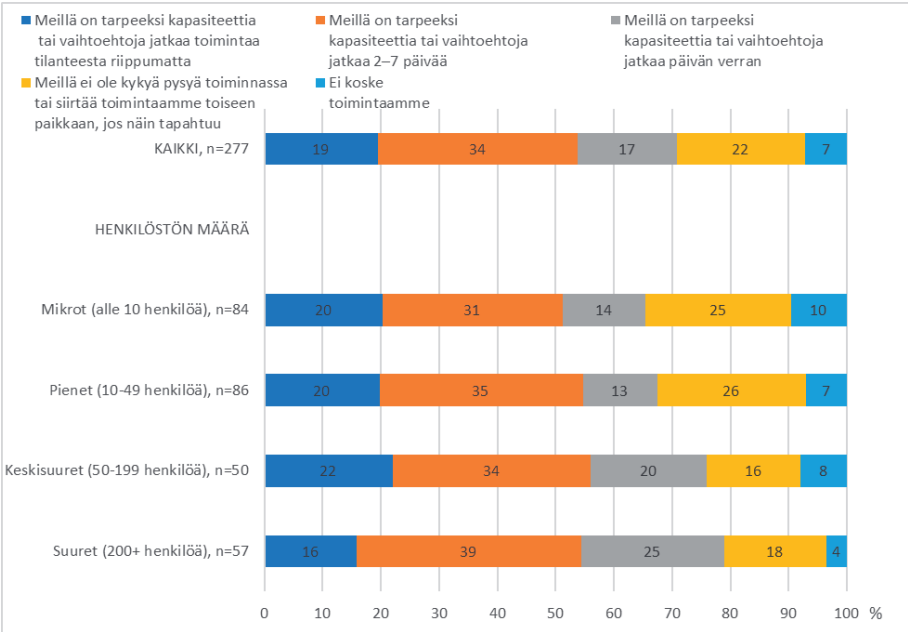
Digitaalisten palvelujen toiminnan estäminen tai estyminen

Viidesosa (22 %) vastaajayrityksistä ei pysty jatkamaan päivääkään ilman digitaalaisia palveluja. Kolmasosa (34 %) kykenee jatkamaan toimintaa 2-7 päivään. Viidesosa (19 %) yrityksistä kykenee jatkamaan toimintaa digitaalisten palvelujen toiminnasta huolimatta. Viidesosa (17 %) selviää päivän verran.

Yli kolmasosa suurista (39 %) ja kolmasosa keskisuurista (34 %) kykenee jatkamaan 2-7 päivään. Kuusitoista (16) prosenttia suurista ja viidesosa keskisuurista (22 %) kykenevät jatkamaan toimintaa ilman tiedostoja.

Kaikista vastaajayrityksistä noin puolet (48 %) on varautunut suunnittelemalla sitä, miten jatkaa toimintaa digitaalisten palvelujen käytön estyttyä. Yli puolet (52 %) vastaajayrityksistä ei siis ole suunnitellut jatkuvuutta digitaalisten palvelujen käytön estyttyä. Moni yritys tarjoaa erilaisia digitaalisia palveluja ja niillä on vaikutus yrityksen kassavirtaan.

Miten hyvin yrityksenne kestää digitaalisten palvelujen estymisen tai estämisen?



JOHTOPÄÄTÖKSET

Hybridivaikuttaminen on lisääntynyt neljän vuoden takaisesta

Yritysten kokema epäilty hybridivaikuttaminen on lisääntynyt viimeisen neljän vuoden aikana. Joka neljäs (23 %) vastaajayritys oli kokenut vaikuttamiseksi epäilemäänsä toimintaa. Kasvua on kolmetoista prosenttiyksikköä vuodesta 2018.

Suurten yritysten kokema vaikuttaminen on kohdistunut kolmasosaan vastaajista. Määrä on kasvanut kaksitoista prosenttiyksikköä (20 % → 32 %) neljässä vuodessa. Hybridivaikuttamisen tunnistaminen on haaste ja on selvää, ettei kaikkia tilanteita tunnisteta. Vieraan valtion operaatiot ovat pitkäkestoisia ja niihin on panostettavissa merkittäviä resursseja.

Yritykset ovat reitti yhteiskunnalliseen päätöksentekoon ja kriittiseen infrastruktuuriin. Kyky tunnistaa vaikuttamista on hybridivaikuttamisen torjunnan kulmakivi. Se vahvistaa puolustautuvan maan suojamuuria ja ennaltaehkäisee vaikuttamisyriityksiä. Tiedonjaon ja koulutuksen lisääminen tukee tämän tavoitteen toteutumista.

Todennäköisyys olla vieraan vallan vaikuttamistoiminnan kohteena

Lähes puolet suurista yrityksistä (47 %) arvioi vaikuttamisen todennäköisyyden olevan vähintään melko todennäköistä. Suuret yritykset ovat näkyviä, niillä on usein laaja asiakaskunta, valtiollisia asiakkaita, suhteita poliittikkoihin, yhteiskunnan infraan liittyviä toimeksiantoja ja muita vastavia tekijöitä joiden kautta ne voivat valikoitua vieraan vallan toiminnan kohteiksi tai reiteiksi lopullisiin kohteisiin.

Aiemmin vuonna 2018 toteutetussa selvityksessä vain kaksi prosenttia suurista vastaajayrityksistä piti vaikuttamisen mahdollisuutta erittäin todennäköisenä.

Neljässä vuodessa kasvua oli tullut kymmenen prosenttiyksikköä kahteentoista prosenttiin.

Yleisimpänä syynä (32%) päätyä vieraan valtion mielenkiinnon kohteeksi vastattiin olevan yrityksen keskeisen ja vakiintuneen aseman yhteiskunnassa. Toiseksi yleisimmäksi syyksi (22%) nousi johdon ja avainhenkilöiden henkilökohtaiset yhteydet johtaviin tai toteuttavan tason viranomaisiin.

Kohdemaan päätöksentekoon vaikuttamaan pyrkivän tahon tarkoituksena on päästä kiinni yritysten kautta tavalla tai toisella poliittiseen päätöksentekoon ja virkamiehiin. Pyrkiessään tähän päämäärään vieras valtio tarvitsee erilaista tietoa, jota yrityksillä on hallussaan tai mihin niillä on pääsy.

Viranomaisilla yhä kirittävää – yritykset kaipaavat tukea ja ovat valmiita yhteistyöhön

Yritykset tuntevat varsin hyvin viranomaiset. Viranomaisilla on yhä hieman kirittävää, tiedon lähteenä ne jäävät toiseksi medialle. Lähes kaikki yritykset (96 %) kaipaavat viranomaisilta tietoa oppaiden ja koulutusten muodossa.

Hybridiuhkien torjuminen edellyttää viranomaisten ja yritysten yhteistyötä. Vaikuttaminen voi aiheuttaa negatiivisia seurauksia sekä valtiolle että yrityksille. Yrityksillä on halukkuutta tehdä yhteistyötä viranomaisten kanssa. Toisaalta ne kaipaavat neuvoja ja koulutusta tunnistaakseen vaikuttamistilanteita. Yritysten keskuudessa on paljon hyödyntämätöntä potentiaalia hybridiuhkien torjuntaan. Tilanteen kehittäminen edellyttää aktiivisuutta viranomaisten puolelta. Niin sanotut ”vihreät miehet” edustavat arviolta viimeistä neljänneistä hybridi-vaikuttamisen ajallisesta kaaresta. Yritykset ovat osana ajallisesti huomattavasti pidempää ja yhteiskunnalliseen päätöksentekoon paljon huomaamattomammin ja haitallisemmin vaikuttavaa osaa hybridi-vaikuttamisesta. Viranomaisen torjuntatyön keskittäminen siihen vaiheeseen olisi demokraattisen päätöksenteon suojaamisen kannalta tehokkaampaa resurssien käyttöä.

Arjessa uhkaava informaatiovaikuttaminen tunnistetaan hyvin

Yritykset tunnistavat varsin hyvin informaatiovaikuttamista (81 %) ja osaltaan siihen vaikuttaa asian avoin käsitleminen julkisuudessa. Medialle on viimeisen vuosikymmenen aikana tullut tärkeä rooli yhteiskunnan informaatiovaikuttamisen vastaisessa toiminnassa.

Informaatiovaikuttamisen tehokkuus perustuu siihen, että suuri osa länsimaiden kansalaisista on tavoitettavissa älypuhelimien ansiosta. Ne kulkevat kaikkialla mukana ja niistä käytetään internetin sivustoja ympäri vuorokauden. Mitä heikompi viranomaisviestintä on kohdemaassa, sitä hedelmällisempi kohde se on vieraille vallalle. Viranomaisilta vaaditaan jatkuvaa valmiutta toteuttaa selkeää ja asiapohjaista vastaviestintää.

Hybridivaikuttamisen seurauksena kansallisen itsenäisyyden tai päätäntävällän rapautuminen

Yritysten mukaan kolme vakavinta seurausta hybridivaikuttamisesta ovat kansallisen itsenäisyyden tai päätäntävällän rapauttaminen (53 %), luottamuksellisten tietojen (yritys tai valtio) menettäminen (52 %) ja vaikutus poliittiseen päätöksen-tekoon (51 %).

Hybridivaikuttamisen tavoitteena voi olla erilaisia asioita. Jotain yhteiskunnallista kehityskulkua voidaan pyrkiä hidastamaan, estämään tai vastavuoroisesti asia-tila pyritään pitämään ennallaan ja toimet valikoituvat sen mukaan. Tässä toiminnassa yritykset voivat olla kohteena, reittinä tai vaikuttamisen alustana. Kaikille näille vaihtoehdoille on yhteistä se, että vieraan valtion edustajat luovat suhteen yritykseen ja pyrkivät sitten toteuttamaan tavoitteitaan eri tavoin.

Vieraiden valtioiden hyödyntämät yritysten heikkoudet

Yritykset tunnistavat hyvin heikkoudet, joita vieraan valtion on helppo hyödyntää operaatioissaan. Yritysten mukaan liika avoimuus ja sinisilmäisyys ovat suurim-

pia heikkouksia (67 %) hybridivaikuttamisen suhteen. Niiden lisäksi puutteellinen kyky tunnistaa (56 %) vaikuttamistilanteita huolettaa yrityksiä. Liiallinen riippuvuus kansainvälisistä palveluista tai osaamisesta (39 %) mahdollistaa painostuksen ja työntekijöiden tietoisuuden ja valppauden puute (35 %) vaikuttaa osaltaan merkittävästi yritysten mahdollisuuksiin tunnistaa hybriditoimintaa.

Syy näiden heikkouksien yleisyyteen on yksinkertaisesti tiedon puute. Ilman tietoa ja osaamista on vaikea toimia turvallisesti ja samalla torjua hybridivaikuttamista. Ratkaisu tilanteen parantamiseksi on viranomaisten aktiivisuuden lisääminen yritysten suuntaan.

Kriittinen vuorokausi ja yritysten jatkuvuus

Yritykset kestävät suhteellisen hyvin niiden käytettävyyden häiriöitä oli sitten kyse sähköstä, tiedostoista, digitaalisista palveluista, vedestä tai jostain muusta toimintaan tarvittavasta asiasta. Vuorokauden jatkuva keskeytyminen muodostaa vedenjakajan, jonka jälkeen toimintaa jatkamaan kykenemättömien yritysten määrä nousee niin korkeaksi, että ainakin alueellisesti se saattaa haitata muiden yritysten toimintaa.

Vuorokauden mittaiset katkot ovat harvinaisia ja ne ovat yleensä paikallisia tai alueellisia. Tahallisesti aiheutettuna vuorokauden mittaisen haitan aiheuttaminen vaatisi usean kohteen toiminnan lamauttamista samanaikaisesti tai porrastetun ja synkronoidun lamauttamisen kautta.

Kassavirran turvaaminen, työntekijöiden palkanmaksun ja työsuhteiden pysyvyyden varmistaminen ovat motiiveja, joiden vuoksi yritykset ovat valmiita kehittämään jatkuvuuttaan ja häiriönkestoaan.

Valtion ja yritysten jatkuvuus on toisistaan riippuvainen kokonaisuus. Ilma toista ei saavuteta riittävää yhteiskunnallista resilienssiä. Siksi laaja-alainen yhteistyö myös hybridiuhkien torjunnassa on ainoa ratkaisu jolla saadaan nostettua yhteiskunnallista resilienssiä.

LISÄTIETOA

City of Helsinki (2018) Helsinki in the era of hybrid threats – Hybrid influencing and the city

Clingendael Institute (2018) Hybrid Conflict: The Roles of Russia, North Korea and China

Clingendael Institute (2018) Hybrid Conflict and the Future European Security Environment

Egmont Institute (2022) Hybrid Warfare Is not Synonymous with Cyber: The Threat of Influence Operations

European Parliament (2021) Best Practices in the whole-of-society approach in countering hybrid threats

Helsingin seudun kauppakamari (2021) Yritysvakoilu 2021 –selvitys

Institute for Strategic Research of the French Ministry for the Armed Forces Paul Charon) and Jean-Baptiste Jeangène Vilmer (2021) Chinese Influence Operations

Keskuskauppakamari ja Helsingin seudun kauppakamari (2017, 2012, 2008 ja 2005) Yritysten rikosturvallisuusriskit ja niiden hallintaselvitykset.

Naeringslivens sikkerhetsråd (2018) The Hybrid Study

Jääskeläinen Ville (2018) Liikesalaisuuksiin kohdistuvien insider-riskien hallinta

Poliisiammattikorkeakoulu (2021) Kyberrikos on poliisiasia Opas yrityksille kyberrikostutinnan kulusta

Sisäministeriö (2017). Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisu 14 / 2017. Helsinki 2017.

Suojelupoliisi (2022) Kansallisen turvallisuuden katsaus 2021

Suojelupoliisi (2022) Vuosikirja 2021: Korkealaatuinen tiedustelutieto on ulko- ja turvallisuuspoliittisessa päätöksenteossa välttämätöntä

Valtioneuvoston kanslian julkaisuja 2019:11, Informaatiovaikuttamiseen vastaaminen : Opas viestijöille

KESKUS-
KAUPPAKAMARI

Keskuskauppakamari, World Trade Center Helsinki,
PL 1000, Aleksanterinkatu 17, 00100 Helsinki | puh. 09 4242 6200
keskuskauppakamari@chamber.fi | @K3FIN
[kauppakamari.fi](https://www.kauppakamari.fi)