Tulevaisuuden kyberturvallisuus ja hybridiuhkat

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus kiittää mahdollisuudesta lausua kyberturvallisuudesta ja hybridiuhkista tulevaisuudessa (O 5/2019 vp Tulevaisuusvaliokunnan selvityshankkeet 2019-2023, Teema: Kyberturvallisuus ja hybridiuhkat tulevaisuudessa). Kyberturvallisuuskeskus keskittyi nostamaan esille kyberturvallisuuden näkökulmasta merkittäväksi muodostuvia kehityskulkuja, jotta niiden muotoutumiseen tai niihin varautumiseen pystytään politiikan keinoin vaikuttamaan. Kaikki nykyiset uhkat ovat myös tulevaisuudessa keskeisiä uhkia. Pidemmän aikavälin seuranta on osoittanut, että tekotavat muuttuvat, mutta kyberuhkien perusolemus muuttuu hitaammin.

Kyberturvallisuuskeskus haluaa nostaa esille keskeisinä tulevaisuuden hybridiuhkien ja kyberturvallisuuden teemoina haitallisten keinojen valikoiman laajuuden, teknologiadisruptiot ja niiden aiheuttamat haasteet uhkia vastaan varautumiseen, monimutkaiset keskinäisriippuvuudet, datan ja tekoälyn vaikutuksen mielipidevaikuttamiseen sekä osaamisen ja koulutuksen tärkeyden. Näistä lisää seuraavassa.

1 Poikkitieteellisyys ja hajaantuneisuus tekevät hybridiuhkista vaikeita riskienhallinnan kohteita

Uusien ja kompleksisempien teknologioiden hyödyntäminen hybridivaikuttamiseen on selvää. Siksi onkin tärkeää tunnistaa keinoja, joilla vaikuttamista voidaan rajata, tai se pystytään havaitsemaan tehokkaasti. Havaitsemisen lisäksi on olennaista, että valtuutetut tahot tietävät miten toimitaan, ja että viranomaisyhteistyö on saumatonta. Hybridivaikuttamisen tilannekuvan muodostaminen on haastavaa, kun pienet häiriötilanteet tapahtuvat eri aloilla, ja tiedonkulku ei ole rutinoitunutta.

Valtioneuvoston kanslian mukaan hybridivaikuttamisella tarkoitetaan vihamielisen valtion Suomeen kohdistamaa ei-toivottua vaikuttamista. Vaikuttaminen voi tapahtua pidemmällä aikavälillä esimerkiksi useaa eri keinoa käyttäen tai samanaikaisesti usealla eri sektorilla.

Kyberulottuvuus tarjoaa laajan toimintakentän hybridivaikuttamiselle ja monissa tapauksissa sitä on hyödynnetty osana isompaa tapahtumaketjua. Suomessa Kyberturvallisuuskeskus saa useita ilmoituksia päivässä ja nämä ovat monesti yksittäisiä tapahtumia, tai esimerkiksi rikollista toimintaa. Ne eivät kuitenkaan liity suurempaan tapahtumaketjuun, jolloin hybridivaikuttamisen elementit täyttyisivät.

Vaikuttamisen välineinä voidaan kyberulottuvuuden lisäksi käyttää esimerkiksi tiedon väärentämistä, mielipidevaikuttamista ja sen polarisaatiota sekä trollaamista, korruptiota, perinteisiä painostuskeinoja, kuten mustamaalaamisen uhkaa tai informaatio-operaatioita.

Kyberturvallisuuskeskus seuraa erilaisia tapahtumia kyberturvallisuuden näkökulmasta, ja tekee laajaa yhteistyötä muiden toimijoiden kanssa sekä valtionhallinnossa että yksityisellä sektorilla. Tarkoituksena on tunnistaa hybridivaikuttamisen ketjuja Suomessa, joissa kyberulottuvuus on osana tapahtumaketjuja. Yhteistyöllä on vahva kansallinen ja kansainvälinen ulottuvuus.

Kaikki kyberhyökkäykset eivät kuitenkaan ole hybridivaikuttamista ja kaikkeen hybridivaikuttamiseen ei liity kyberelementtiä. Hybridivaikuttajan tärkein

tietovaranto onkin löytää kohdeyhteiskunnan heikkoudet ja haavoittuvuudet, ja hyödyntää niitä vastaan sopivinta keinovalikoimaa.

2 Teknologisen kehityksen nopeus haastaa hybridivaikuttamista vastaan varautumisen

Suurvaltiot ovat osoittaneet jatkuvan kiinnostuksensa uusiin teknologioihin, kuten 5G, big data ja tekoäly. Esimerkiksi big datan kohdalla ns. Cambridge Analytica –tapauksen suhteen on esitetty arvioita, että tapaus on kiinnostanut vieraita valtioita myös pahantahtoisessa toiminnassa. Tulevaisuudessa vieraat valtiot selvittävät eri teknologioiden mahdollisuudet vaikuttamiseen. Mahdollisesti niitä otetaan myös pahantahtoiseen käyttöön strategisten tarpeiden mukaisesti.

Kehittyvien ja tulevaisuuden teknologioiden käyttöönotto tapahtuu nopeasti. Tällaisia teknologioita ovat esimerkiksi **5G**, 6G, **tekoäly** ja **kvanttilaskenta**. Riskien tunnistamattomuus jättää mahdollisuuden rikollisille ja vihamielisille toimijoille tehdä kartoitusta mahdollisten tietoturvallisuusaukkojen löytämiseksi ja niiden hyödyntämiseksi esimerkiksi tiedon varastamiseksi tai järjestelmien manipuloimiseksi.

Koska uudet teknologiat koskettavat laajoja yhteiskunnan osa-alueita, potentiaalinen hyökkäyspinta-ala kasvaa ja tunnistamattomien riskien ennakoiminen on mahdotonta. Uudet teknologiat tulevat muuttamaan ja tuomaan riippuvuuden teknologiasta ihmisten jokapäiväiseen elämään esimerkiksi älyliikenteen ja esineiden internetin myötä. Älykkäitä kuntia rakennetaan parhaillaan ja turvallisuusnäkökulma tulisi huomioida ratkaisuja valittaessa, koska ne vaikuttavat myös kansalaisiin ja yhteiskunnan toimintaan normaaliajassa sekä poikkeusoloissa.

Suomessa julkaistaan marraskuussa tietoturvamerkki, joka myönnetään tuotteille jotka ovat hyvin suojattuja yleisimmiltä kuluttajaan kohdistuvilta tietoturvauhkilta. Vuoden 2019 maaliskuussa julkaistussa European Cyber Security Actissa on sama ajatus, mutta jaottelu on kolmiportainen (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN).

Uusiin keskeisiin teknologioihin tulee varautua kansallisilla ja EU-tasoisilla riskianalyyseillä, kuten on jo osin tehty 5G-teknologian osalta. Tästä pitäisi kuitenkin saada jatkuva malli, joka asettaa koko EU-alueen teknologian varteenotettavaksi markkina-alueeksi, antaen EU-maiden turvallisuusvaatimuksille painoarvoa. EU-laajuisesti sovitut puitejärjestelyt ovat globaalien suuryritysten kiinnostuksen kohteina. Tietoturvamerkki tai vastaava, joka myönnetään globaalille toimijalle tai sen palvelulle, on markkinaetu. Suomen tietoturvamerkki on hyvä osoitus mitä kansallisella tasolla voidaan tehdä tietoturvallisuuden varmistamisessa.

3 Keskinäisriippuvaisuudet kyberturvallisuuden monimutkaistajana

Digitalisaatio ja globalisaatio kulkevat käsi kädessä keskinäisriippuvaisuuksien kasvun kanssa. Joustava ja ennakoiva riskienhallinta sekä kansallisen turvallisuuden takaava sääntely korostuvat tässä ympäristössä.

Teknologian, infrastruktuurin ja palveluiden keskinäisriippuvuuksilla tarkoitetaan eri toimijoiden riippuvuutta toisesta. Esimerkiksi matkaviestintäverkot eivät toimi ilman tukiasemia, jotka eivät toimi ilman sähköä. Useimpia sähkölaitoksia ja sähköverkkoja ohjataan viestintäverkkoja ja tietojärjestelmiä käyttäen. Edellä mainitut keskinäisriippuvuudet ovat hallitseva tekijä yhteiskunnan kriittisissä toiminnoissa. Edellä mainittujen keskinäisriippuvuuksien päällä tulee olemaan

monta digitaalisen yhteiskunnan palvelua kuten älyliikenne ja terveydenhuollon uudet palvelut jotka ovat tärkeitä elementtejä ilmastonmuutoksen vastaisessa toiminnassa sekä yhteiskunnan rakenteen muuttuessa.

Haasteena on keskinäisriippuvuuksien kartoittaminen ja niihin liittyvien riskien minimointi. Lisäksi keskinäisriippuvuudet tulisi ymmärtää myös niihin tukeutuvien palveluiden kannalta. Keskeisenä kysymyksenä kartoituksessa on ymmärtää mihin palveluihin ja kuinka suuri vaikutus kansalaisiin ja yhteiskuntaan on toteutuvalla riskillä. Esimerkiksi viranomaispalveluista moni on riippuvainen suomi.fi-tunnistautumisesta.

Kun uutta teknologiaa ja uusia palveluita kehitetään olemassa olevien järjestelmien päälle, vanhojen osien päivittämien tai korvaaminen saattaa kaataa koko järjestelmän. Elinkaaren hallinta on tärkeää kokonaisuuden kannalta, sillä virheet sen kohdalla altistavat uudenkin järjestelmän vanhoille tietoturvallisuusuhkille. Yhteiskunnassa käytössä olevien teknologioiden elinkaari on kasvanut huomattavasti, esimerkiksi ensimmäiset 2G-verkot tulivat käyttöön 1990-luvun aikana ja niiden arvioitu elinkaari on noin 40 vuotta. Pitkän elinkaaren tekniikka on yleensä haavoittuvimmillaan elinkaaren loppuvaiheilla, jos riskialttiita ohjelmistoja ei korjata vastaamaan ajantasaisia turvallisuusvaatimuksia.

Kerrannaisvaikutukset saattavat ilmaantua normaaliolojen häiriötilanteessa, esimerkiksi voimakkaan myrskyn aikana, tai kyberhyökkäyksen yhteydessä. Tapahtunut häiriö kohdistuu yhteen paikkaan mutta vaikutukset saattavat näkyä toisessakin palvelussa ikään kuin sivuosumana. Riskikartoituksen mahdollisuus tunnistaa näitä voi olla erittäin vaikeaa. Kasvava kompleksisuus kasvattaa hyökkäyspinta-alaa myös sellaisiin suuntiin, joihin perinteisellä elinkaarenhallinnalla ei osata varautua.

Myös pilviteknologioiden ja -palveluiden yleistyminen altistavat uusille uhkille - useimmat edellisen sukupolven uhkakuvat ovat edelleen ajankohtaisia myös pilvipalveluissa. Pilvipalveluissa tieto ei enää ole välttämättä yhden maantieteellisen alueen sisällä. Tällöin vaikuttaminen saattaa tapahtua maantieteellisesti siellä, missä havainnointikyky ei ole hyvällä tasolla, tai mahdollisen tiedon luottamuksellisuuden menetyksen havaitseminen ei ole mahdollista. Palvelinkeskusten maantieteellinen hajanaisuus voi mahdollistaa ei-toivotun tiedonhankinnan tai tiedon manipuloinnin.

4 Kyberavaruus on tiedustelutoiminnan ja hybridivaikuttamisen pelikenttää

Kybertiedustelu tulee olemaan tulevaisuudessa hybridivaikuttamisen väline. Sen tärkeimpinä tavoitteina on kerätä tietoa sekä yrityssalaisuuksista, uusista innovaatioista ja tutkimustoiminnasta, investoinneista sekä päätöksenteosta ja muusta valtionhallinnon virkatoiminnasta.

Kybertiedustelun haasteena on jo aiemmin mainittu attribuutio. Sen lisäksi, että kyberulottuvuudessa on helppoa piilottaa omat jälkensä, monen valtiollisen toimijan tiedetään käyttävän niin sanottuja proxyjä, eli välikäsiä toimiensa toteuttajana. Välikäsien lisäksi myös terroristijärjestöt ja ei-valtiolliset toimijat hyödyntävät kyberulottuvuutta toimintaansa. Vaikka ei-valtiolliset toimijat, rikollisryhmittymät ja välikädet eivät kuulu valtioneuvoston kanslian käyttämään määritelmään, on ne kuitenkin hyvä huomioida puhuttaessa kyberturvallisuudesta ja kyberulottuvuudesta hybridivaikuttamisen toimintakenttänä.

Rahallisten intressien ja investointien seuraaminen ja tiedon kerääminen kybertiedustelun keinoin jatkuu. Mitä enemmän ulkomaisia investointeja on, sitä enemmän tiedustelu lisääntyy. Ulkomaisessa valtaomistuksessa olevien yritysten

investointien (kriittisen infrastruktuurin kohteet, tieto- ja viestintäteknologia, yms.) toteuttamista valvotaan rahoittajien toimesta. Myös tulevaisuuden suuret kansalliset investoinnit varmasti herättävät ulkovalloissa kiinnostusta. Tulevaisuudessa kyberulottuvuuden kautta kohdistetaan tiedustelua enenevissä määrin yksityishenkilöihin. On todennäköistä, että yhä useammat valtiot hyödyntävät kybertiedustelua keinovalikoimassaan.

Kybertiedusteluun varautumisessa olennaista on organisaation oma havainnointikyky, sekä mahdollisimman alhainen ilmoituskynnys asiaa keskitetysti tutkiville viranomaisille. Esimerkiksi Kyberturvallisuuskeskus muodostaa kansallista kyberturvallisuuden tilannekuvaa pääosin sille vapaaehtoisesti tehtyjen ilmoitusten nojalla.

5 Hybridihyökkääjän tavoitteena on usein mielipidevaikuttaminen

Hybridivaikuttamisella pyritään valtioiden ja yksityisten yritysten lisäksi vaikuttamana myös yksittäisiin kansalaisiin, ja heidän mielipiteeseen. Mielipidevaikuttaminen on erityisesti sosiaalisen median kautta helppoa, ja jälkien peittäminen yksinkertaista.

Paljon esillä ollut trollaaminen, sosiaalisen median kautta tehtävä mielipidevaikuttaminen, algoritmien käyttö mainonnan ja viestien kohdentamiseen sekä deep fake -ilmiö mielletään monesti kyberuhkaksi. Deep fake -termillä tarkoitetaan tapaa tehdä muokattuja videoita tekoälyä ja koneoppimista käyttäen. Tämä mahdollistaa henkilön liittämisen videoon jossa hän ei ole itse ollut tai saada henkilön käyttäytymistä videolla muuttumaan oleellisesti. Tekoäly pystyy käyttämään henkilön ennalta nauhoitettuja ääntä, kasvokuvia tai videoita uuden väärennetyn videon lähdeaineistona.

Tulevaisuutta silmällä pitäen on syytä pohtia disinformaation hallinnan tulevaisuutta erityisesti alustaekosysteemien, tiedon jakamisen ja jäljitettävyyden näkökannalta sekä faktan-tarkistuksen roolia. Teknologian nopea kehitys avaa aivan uudenlaisia mahdollisuuksia sekä hallita tietoa, säännellä tietoa viranomaisten toimesta ja toisaalta teknologinen kehitys antaa mahdollisuuden levittää disinformaatiota entistä nopeammin ja tehokkaammin. Disinformaation tuottamisen lisäksi tekoälyä voitaisiin tulevaisuudessa käyttää faktantarkastamiseen ja disinformaation tunnistamiseen. Media-alustat voivat tulevaisuudessa kehittyä interaktiivisemmaksi ja tätä kautta kuluttajalle voitaisiin antaa mahdollisuus räätälöidä itse itselleen sopivia sisältöjä keinoälyn avulla. Lohkoketjuteknologia voisi tarjota tulevaisuudessa parempaa tiedon läpinäkyvyyttä ja jäljitettävyyttä. (Euroopan komissio 2018, 11-12.) Tekoäly voisi muokata paremmin oppivia algoritmeja, joita voisi hallita itse tai voisi tutkia datalähteiden paikansapitävyyttä. Tekoälyn, koneoppimisen ja virtuaalitodellisuuden mahdollisuudet ovat huikeat disinformaation torjumiseksi. Kuluttajan kannalta on tärkeää saada teknologia tuottamaan innovatiivisia ratkaisuja väärennetyn tiedon torjumiseksi.

Esimerkiksi deep fake -konseptiin perustuvan teknologian kehitys ja käyttö on kasvanut nopeasti ja siitä on oletettavissa hyvin merkittävä uhka mielipidevaikuttamiseen sen helppokäyttöisyyden vuoksi. Älypuhelimille on jo nyt saatavissa helppokäyttöisiä, mutta hyvin alkeellisia deep fake sovelluksia kuten kiinalainen Zao.

Kyberturvallisuuskeskuksen näkökulman ja toimivallan mukaan mielipidevaikuttaminen ei ole tekninen tietoturvaongelma eikä kuulu Kyberturvallisuuskeskuksen toimialueelle. Olisi hyvä tarkastella mikä toimija

Suomessa pystyisi parhaiten seuraamaan ja puuttumaan edellä mainittujen informaatioympäristön vaikuttamisyrityksiin.

Vaalihäirintä pysyy hybridivaikuttamisen keinona

Vaaleissa ihmisille rakennetaan mielikuvia, jolloin mielipidevaikuttaminen on todella helppoa ja tehokasta. Mielipidevaikuttamisella voidaan kääntää vaalitulosta haluttuun suuntaan. Tästä on runsaasti esimerkkejä viimeiseltä vuosilta niin kansainvälisesti kuin kansallisesti. Kaikki uutisointi ja raportoidut hyökkäykset saattavat vaikuttaa kansalaisten luottamukseen ja turvallisuuden tunteeseen, mikä puolestaan pahimmillaan vaikuttaa demokraattiseen prosessiin.

Jatkuvasta hyvästä varautumisen tasosta huolimatta vaalihäirintä tulee olemaan hybridivaikuttamisen potentiaalinen kohde myös tulevaisuudessa. Tällä hetkellä Suomessa luotetaan lippuäänestykseen, jolloin vaalitulokseen vaikuttaminen on mahdotonta. Tästä huolimatta hybridivaikuttamisen keinovalikoima mahdollistaa muun vaaleihin yhdistetyn häirinnän, kuten edellä mainitun mielipidevaikuttamisen.

6 Koulutus, osaaminen ja tutkimustoiminta pitkän aikavälin varautumiskeinoja

Osaaminen

Global Information Security Workforcen tekemän tutkimuksen mukaan pelkästään Euroopassa tulee olemaan vuoteen 2022 mennessä 350 000 kyberturvallisuusammattilaisen saatavuusvaje. Kyberturvallisuuskulttuurin rakentuminen on koulutuskysymys, ja sen rakentamisessa tulisi huomioida järjestelmien koko elinkaari suunnittelemisesta ja ohjelmistokehityksestä alkaen.

Uusien osaajien hankinnassa on kuitenkin hyvä pitää kiinni hyvistä käytännöistä, vaikka tekijöiden puute saattaisi houkutella nopeuttamaan ja keventämään prosessia. Maailmalla puhutaan niin sanotusta insider threat -ilmiöstä. Tällä tarkoitetaan organisaation oman henkilöstön toiminnasta aiheutuvaa uhkaa. Osaajien puute voi helpottaa huoltovarmuuskriittisten organisaatioiden työntekijäksi soluttautumista. Olisi hyvä pohtia millä keinoin turvallisuusselvitysten ja muiden turvallisuuteen liittyvien prosessien läpimenoa voitaisiin tehostaa.

Koulutus

Korkeakoulut pystyvät reagoimaan osaamisvajeeseen, mutta tämä edellyttää julkisen ja yksityisen sektorin vuoropuhelua. Suuri osa Suomen kansalaisista on työikäistä väestöä, jota koulutus ei kuitenkaan tavoita. Tämän osaamisen kehittämisessä työnantajat ovat keskiössä. Työntekijöillä tulee olla tarvittavaa osaamista, jotta he voivat toimia kyberturvallisesti työssään.

Kyberturvallisuus ja hybridivaikuttamisen havaitseminen ovat nykypäivän kansalaistaitoja. Tällä hetkellä kyber- ja hybridiuhkien kytkeminen arkipäivään on hankalaa. Tällä hetkellä kolmas sektori on ainoa taho, joka tarjoaa koulutusta kaikenikäisille kansalaisille. Koulutus nähdään keskeisenä osana kansallisen resilienssin kasvattamiselle ja siksi siihen panostaminen olisi tärkeää.

Hallinnon tulisi kouluttaa lisäksi itseään. Virkamiehistö näkee informaatiovaikuttamisen virkatehtäviensä puitteissa varhaisessa vaiheessa. Tällä hetkellä esimerkiksi hybridivaikuttamista ja kyberulottuvuutta sen osana ei tunnisteta osaamispuutteiden vuoksi. Mikäli henkilöstö ei tunnista

vaikuttamisyritystä, ovat seuraukset ei-toivotut. Tämä vaikuttaa tilannekuvan muodostamiseen.

Tutkimustoiminta

Tutkimuksella tulee tunnistaa ja ennakoida kybertoimintaympäristön kehityskulkuja, jotta niitä voidaan kehittää ennakoivasti kehittyvää teknologiaa vastaavaksi. Tutkimuksella edistetään kotimaisen kyberosaamisen pitkäjänteistä kehittämistä ja osaamisen huoltovarmuutta.

Pienyritysten ja tutkimusverkostojen varhaisella mukaan ottamisella päätöksentekoon riskejä tunnistettaisiin jo etukäteen. Lisäksi Suomen on tärkeää aktiivisesti edesauttaa näiden toimijoiden osallistumista hybridiuhkiin liittyvään keskusteluun. Toimijapohjan laajuus edesauttaa hiljaisten signaalien tunnistamista ja näin ollen auttaa proaktiivisessa varautumisessa tulevaisuuden teknologioita käyttöönotettaessa. Tutkimustoiminta pystyy reagoimaan nopeasti muutoksiin ja hiljaisiin signaaleihin, ja tuottamaan tietoa valtionhallinnon päätöksenteon tueksi.

Kansallisen tutkimuksen lisäksi on tärkeää osallistua kansainväliseen tutkimustoimintaan sekä esimerkiksi EU:n omien tutkimuslaitosten työhön. Osana kansainvälistä tutkimustoimintaa Suomi voi vaikuttaa EU:n päätöksentekoon esimerkiksi uusien teknologioiden hyödyntämisestä.

7 Tilannekuvan muodostaminen on kriittistä

Kyberulottuvuus osana hybridivaikuttamista on laaja pelikenttä. Nopeasti muuttuvassa maailmassa tilannekuvan ja tapahtumien liittäminen toisiinsa on haastavaa ja siksi myös hybridivaikuttamisen tunnistaminen on vaikeaa.

Hybridivaikuttaminen tapahtuu lähes aina sellaisen rajan tai kynnyksen alapuolella, joka menee yksittäisten viranomaisten toimivallan alle. Viranomaiset eivät jaa aktiivisesti tietoa, koska tilanne ei vaadi poikkihallinnollista yhteistyötä. Näin ollen kokonaistilanne jää hahmottamatta, eikä hybridivaikuttamista voida tunnistaa.

Valtionhallinnossa ja yksityisellä sektorilla tehdään valtavasti hyvää yhteistyötä. Haasteen yhteistyöhön muodostaa se, että sitä tehdään eri tasoilla, mutta tieto ei kulje niiden välillä. Operatiivista tietoa ei osata tunnistaa strategisesti merkittäväksi ja toisinpäin. Poikkihallinnolliset verkostot, tilannekuvaa vaihtavat ryhmät sekä asioihin perehtyneet asiantuntijat voisivat edistää yhdessä keskeisten asioiden esille nostamista ja yleistämistä niin, että kokonaiskuva saataisiin kohdennettua oikealla tavalla oikealle yleisölle.

Traficomin tulevaisuustyön tehtävänä on kartoittaa digiyhteiskunnan ilmiöitä, tuottaa tietoa päätöksenteon tueksi, ehdottaa toimenpiteitä, tehdä myös konkreettisia ratkaisuita ja kokeiluja, jotta osaamme paremmin varautua tulevaisuuteen. Tulevaisuustyön yksi konkreettinen tehtävä on kartoittaa ja tunnistaa riskejä tulevaisuuden keskeisissä teknologioissa sekä ymmärtää niiden aiheuttamat muutokset yhteiskunnassa. Käsiteltävät uudet teknologiat ja aiheet tuovat myös uusia näkökulmia ja ilmiöitä hybridivaikuttamiseen.