Dnro TRAFICOM/157822/03.03.01/2025

PuV@eduskunta.fi

Viite: VNS 9/2024 vp

Valtioneuvoston puolustusselonteko

Puolustusvaliokunta on pyytänyt Liikenne- ja viestintävirastolta kirjallista ja suullista lausuntoa valtioneuvoston puolustusselonteosta (informaatioturvallisuus). Liikenne- ja viestintävirasto kiittää mahdollisuudesta lausua asiassa. Liikenne- ja viestintävirasto pitää selontekoa kattavasti valmisteltuna ja toteaa selonteon painopisteiden ja tavoitteiden vastaavan muuttunutta toimintaympäristöä. Liikenne- ja viestintävirasto lausuu selonteosta seuraavaa:

Informaatioympäristö on aina ollut tärkeä vallankäytön ja vaikuttamisen alue. Se ei ole muuttumaton, vaan kehittyy ja muuntuu jatkuvasti muun muassa geopoliittisten, taloudellisten, sosiaalisten, historiallisten, teknologisten ja kulttuuristen tekijöiden vaikutuksesta. Vaikka vaikuttamisen tavoitteet ja psykologisen manipuloinnin keinot ovat pysyneet samoina, teknologian kehitys on läpi historian mahdollistanut yhä tehokkaampia tapoja yhteiskuntaa vahingoittamaan pyrkivälle haitalliselle vaikuttamistoiminnalle.

Nopean teknologisen kehityksen myötä ulkopuolisille pahantahtoisille toimijoille tarjoutuu uudenlaisia ja entistä tehokkaampia ja vaikeammin torjuttavia keinoja horjuttaa yhteiskuntaa. Vaikuttamistoiminta ei rajaudu pelkästään sotilaallisiin konflikteihin, vaan vaikuttamistoimintaa tapahtuu myös normaalioloissa. Tämä edellyttää jatkuvaa yhteiskunnan eri sektorien osaamisen ja valmiuksien kehittämistä tunnistaa, suojautua ja vastata vihamieliseen informaatiovaikuttamiseen.

Kyber- ja informaatiovaikuttaminen tukevat toisiaan

Nykyaikaisessa digitaalisessa yhteiskunnassa ja toimintaympäristössä kyber- ja informaatiovaikuttaminen muodostavat toisiaan tukevan kokonaisuuden ja keinovalikoiman, joita ulkopuoliset toimijat voivat hyödyntää pyrkiessään horjuttamaan suomalaista yhteiskuntaa, demokratiaa, instituutioita ja yhteiskuntarauhaa sekä vaikuttamaan Suomen kansainväliseen yhteistyöhön ja liittolaissuhteisiin sekä maakuvaan. Molemmissa toimintaympäristöissä tapahtuvalla vaikuttamistoiminnalla voidaan pyrkiä aiheuttamaan epävarmuutta yhteiskunnassa tai rapauttamaan suuren yleisön luottamusta organisaatioihin ja laajemminkin informaatioympäristöön ja digitaaliseen yhteiskuntaan erilaisissa turvallisuustilanteissa.

Liikenne- ja viestintävirasto korostaa kyber- ja informaatioympäristöjen välisen vuorovaikutuksen ja yhteisen vaikuttamispotentiaalin ymmärtämistä ennakoitaessa ja varauduttaessa tulevaisuuden uhkiin. Kyberhyökkäykset voivat lisätä informaatiovaikuttamisen mahdollisuuksia sekä psykologisia vaikutuksia. Samalla tavoin kyberhyökkäykset voivat tukea informaatiovaikuttamisen vaikutuksia yhteiskunnassa ja väestön keskuudessa. Manipulaatio, harhaanjohtaminen ja häirintä ovat molemmissa ympäristöissä käytettyjä keinoja. Kyber- ja informaatiovaikuttamisoperaatioiden välinen "kumppanuus" voidaankin jaotella seuraavasti 1. kyberhyökkäykset

informaatiovaikuttamisen keinona itsessään, 2. kyberhyökkäykset informaatiovaikuttamisoperaation tukena tai osana 3. informaatiovaikuttamisen keinojen hyödyntäminen kyberhyökkäyksen käynnistämisessä. Tekoälyteknologioiden avulla luodut deepfake-sisällöt yhdistävät näitä vaikuttamistapoja entistä vahvemmin toisiinsa. Kybermaailman teot voivat olla myös informaatiovaikuttamista.

Informaatioturvallisuuden kehittäminen edellyttää jatkuvaa ja strategista otetta

Puolustusselonteossa tuodaan hyvin esiin informaatiopuolustuksen merkitys ja rooli osana Suomen puolustuskykyä ja -valmiutta. Informaatiovaikuttamisen tunnistaminen ja siihen vastaaminen nähdään yhteiskunnan läpileikkaavana toimintona. Lisäksi vaikuttamiseen varautumisen ja vastaamisen yhteys kokonaisturvallisuuden malliin on nostettu esiin.

Suomalaisen yhteiskunnan kokonaisturvallisuuden jatkuva kehittäminen ja ylläpitäminen edellyttävät sitä, että yhteiskunnan eri sektorit kehittävät jatkuvasti valmiuksiaan varautua, tunnistaa ja vastata normaalioloissa tapahtuviin vihamielisiin ulkopuolisiin vaikuttamisyrityksiin. Lisäksi tarvitaan yhteistyön, tilannekuvan ja tiedonkulun, koordinaation, resursoinnin sekä toimintamallien ja -käytäntöjen vahvistamista. Informaatioturvallisuuden kehittämisessä tulee tehdä tiivistä kansainvälistä yhteistyötä ja tiedonvaihtoa. Liikenne- ja viestintävirasto muistuttaa, että informaatioympäristön uhkiin varauduttaessa ja vastaamisessa on muistettava myös laajemman kansalaisyhteiskunnan merkitys julkisen sektorin ja yritysten lisäksi. Lisäksi moniäänisellä, itsenäisellä ja riippumattomalla journalistisella medialla on nykyisessä informaatiotulvassa entistä keskeisempi rooli yhteiskunnallisen informaatioresilienssin ja demokratian vahvistajana ja ylläpitäjänä.

Liikenne- ja viestintävirasto pitää kannatettavana selonteossa mainittua kansallisen informaatioturvallisuuden konseptin laatimista. Virasto nostaa kuitenkin esiin informaatioturvallisuuden laajemman strategisemman kehittämisen tarpeen Suomessa. Informaatioturvallisuuden yleinen kehittäminen Suomessa vaatii strategista ja kokonaisvaltaista otetta, joka kattaa kaikki yhteiskunnan eri sektorit.

Informaatioturvallisuuden ylläpitäminen ja kehittäminen rakentuu kolmelle osa-alueelle

Viraston näkemyksen mukaan puolustusselonteossa voitaisiin tarkastella laajemmin ja läpileikkaavammin informaatioympäristön uhkia ja niiden vaikutuksia erityisesti henkisen kriisinkestävyyden näkökulmasta. Teknologioita väärinkäyttämällä sekä manipuloimalla ja saastuttamalla informaatioympäristöä esimerkiksi disinformaatiolla, voidaan pyrkiä vaikuttamaan hyvinkin kohdennetusti ja vaikuttavasti erilaisiin väestöryhmiin niin normaali- kuin poikkeusoloissa heikentäen yhteiskuntaa suojelevaa ja koossa pitävää luottamusta. Suomen puolustuskyvyn kannalta tärkeää henkistä kriisinkestävyyttä rakennetaan ja ylläpidetään yhteiskunnassa joka päivä. Siksi informaatioturvallisuutta kehitettäessä on tärkeä pohtia, miten yksiöiden ja yhteisöjen henkistä kriisinkestävyyttä ja informaatioresilienssiä voidaan vahvistaa.

Viraston näkemyksen mukaan informaatioturvallisuuden kehittäminen rakentuu kolmelle osa-alueelle: operatiiviselle, hallinnolliselle ja yhteiskunnalliselle ulottuvuudelle, jotka ovat tiiviissä vuorovaikutuksessa keskenään. Viranomaisten operatiiviset valmiudet ja kyvykkyydet, kuten yhteistyö tilannekuvan ja -analyysin tuottamisessa sekä strategisen viestinnän koordinaatio ja päivittäinen operatiivinen toiminta ovat tärkeitä, mutta yhtä tärkeitä ovat hallinnollisten

kysymysten, kuten lainsäädännön (ml. KV-lainsäädäntö), resurssien ja toimivaltuuksien jatkuva tarkastelu ja kehittäminen nopeasti muuttuvassa informaatio- ja toimintaympäristössä.

Lisäksi on muistettava yhteiskunnan henkisen kriisinkestävyyden ja informaatioresilienssin vahvistamisen merkitys. Koulutus, kulttuuri ja sivistys sekä kansalaisten luottamuksen säilyttäminen suomalaiseen yhteiskuntaan, instituutioihin, mediaan, oikeusvaltioon ja demokratiaan ovat tärkeitä tekijöitä. Luottamus syntyy kansalaisten omakohtaisista kokemuksista perusoikeuksien, osallisuuden ja tasapuolisuuden toteutumiseen. Kehitettäessä informaatioturvallisuutta, on huomioitava kaikkien näiden osa-alueiden merkitys ja vuorovaikutus.

Informaatioturvallisuuden kokonaisuudessa demokraattisessa yhteiskunnassa eri toimijoilla ja instituutioilla on oma roolinsa, tehtävänsä ja rajansa. Informaatioturvallisuutta kehitettäessä on tärkeä varmistaa, etteivät suunnitellut toimintamallit ja toimenpiteet rajoita perusoikeuksia, kuten sananvapautta ja lehdistönvapautta.

Teknologinen kehitys muuttaa informaatioturvallisuuden uhkakenttää

Informaatioturvallisuuden kehittämisessä on tärkeä tunnistaa nopea teknologinen kehitys ja sitä myöten teknologisten suorituskykyjen kasvu. Tämä muutos muuntaa nopealla vauhdilla digitaalisessa toimintaympäristössä tapahtuvaa kyber- ja informaatiovaikuttamista ja lisää entisestään molempien toimintaympäristöjen välisiä yhteyksiä.

Helposti käyttöönotettavat ja käytettävät uudet teknologiat, kuten erilaiset generatiiviset tekoälysovellukset laskevat uusien toimijoiden kynnystä lähteä mukaan vaikuttamistoimintaan. Lisäksi ne muuttavat ja tehostavat jo olemassa olevia vaikuttamisen tekniikoita ja keinoja. Informaatiovaikuttamistoiminnassa tekoäly mahdollistaa ajallisten rajoitteiden poistuminen, hyökkäyksen kohdistamisen useisiin kohteisiin samanaikaisesti sekä hyökkäysteen laajuuden, kattavuuden ja nopeuden ja keston lisäämisen. Tekoälyteknologiat voivat myös auttaa peittämään entistä tehokkaammin vaikuttamistoiminnan taustalla olevan todellisen toimijan tai lavastamaan toimijaksi syyttömän tahon. Lisäksi ne voivat hämärtää kohdeorganisaation tai -yhteiskunnan tilannekuvaa ja vaikeuttaa siten kykyä hahmottaa tai ymmärtää tapahtumia ja tehdä päätöksiä. Lisäksi teknologiat auttavat ennakoimaan kohteen vastatoimenpiteitä sekä analysoimaan ja löytämään suuresta datamäärästä entistä tehokkaammin ja nopeammin kohdeorganisaatiosta/-yhteiskunnasta haavoittuvuuksia. Näitä tietoja voidaan hyödyntää hyökkäyksen valmistelussa sekä tavoitteiden saavuttamisessa.

Jotta yhteiskunnan eri sektorit pystyvät varautumaan ja vastaamaan uudenlaisiin digitaalisessa toimintaympäristössä nouseviin uhkiin, tämä edellyttää jatkuvaa yhteistyötä mm. TKI-toiminnassa. Myös yhteiskunnan henkiseen kriisinkestävyyteen sekä kansalaisten teknologia- ja medialukutaitoon tulee panostaa. Teknologinen kehitys korostaa entisestään tarvetta tarkastella informaatioturvallisuutta operatiivisen tason lisäksi myös strategisemmalla tasolla.

Uhkista keskusteltaessa on hyvä muistaa, että uusia teknologioita voidaan hyödyntää myös puolustuksessa. Teknologiat auttavat tunnistamaan ja analysoimaan mahdollisia hyökkäyksiä ja tarjoamaan työkaluja tunnistaa esimerkiksi tekoälyteknologioiden avulla tuotettuja valheellisia aidon oloisia ja uskottavia Deepfake-sisältöjä. Tämän vuoksi informaatioturvallisuuden kehittämisessä on panostettava uusien teknologioiden kehittämiseen ja hyödyntämiseen sekä niitä koskevaan osaamisen leviämisen yhteiskunnan eri sektoreilla.

Yhteenvetona

Informaatioturvallisuuden kehittämistä tulee jatkaa strategisella otteella tavoitteellisesti ottaen huomioon yhteiskunnan eri sektorit ja niiden tarpeet. Tavoitteena tulisi olla lisätä yhteiskunnan eri sektorien sekä kansalaisten valmiuksia tunnistaa, suojautua ja vastata eri turvallisuustilanteissa Suomeen kohdistuvaan vihamieliseen ulkopuoliseen vaikuttamistoimintaan digitaalisissa ympäristöissä. Informaatioturvallisuus tulee nähdä entistä tärkeämpänä osana kansallisen turvallisuuden kokonaisuudessa. Hyvänä mallina informaatioturvallisuuden kehittämiselle ja vahvistamiselle on pitkäjänteisesti ja strategisesti toteutettu Suomen kyberturvallisuuden kehittäminen.

Viraston näkemyksen mukaan yhteiskunnan läpileikkaavan informaatioturvallisuuden ja -resilienssin strateginen vahvistaminen ja kehittäminen normaalioloissa tukee yhteiskunnan elintärkeiden toimintojen turvaamista ja laajemminkin kokonaisturvallisuutta. Lisäksi se tukee varautumista ja yhteiskunnan eri sektorien kykyä vastata turvallisuustilanteen mahdollisiin nopeisiin muutoksiin. Virasto nostaa lisäksi esiin aktiivisen ja tavoitteellisen kansallisen vaikuttamistyön merkityksen kansainvälistä (esim. EU-tason) sääntelyä kehitettäessä.

Jussi Toivanen
Viestintäpäällikkö
Liikenne- ja viestintävirasto Traficom