

Turvaselonteko: Verkkohyökkäykset konkreettinen uhka

23.1.2009 15:27

Suomen ulkopoliittisen johdon tänään hyväksymä uusi turvallisuus- ja puolustuspoliittinen selonteko ottaa monin paikoin kantaa myös tietoverkkouhkiin.

[Lähes puolitoista vuotta valmisteltu selonteko](#) (pdf) korvaa vuodelta 2004 peräisin olevan vanhan selonteon.

Tähän uutiseen on koottu poimintoja uuden selonteon tietoverkkouhkia koskevista toteamuksista.

Uudessa selonteossa pohjustetaan muun muassa, että sotilaallisten turvallisuusuhkien lisäksi on syntynyt uusia uhkia: Viron ja Georgian kokemukset osoittavat selonteon mukaan, että "tietoverkkohyökkäykset ovat konkreettinen turvallisuusuhka".

"Sähköiset viestintä- ja tietojärjestelmät tehostavat positiivisella tavalla sekä siviili- että sotilastoimintaa. Samalla järjestelmien rakenteet mahdollistavat niiden käytön rikollisiin tarkoituksiin sekä vaikuttamisen yhteiskunnan elintärkeisiin toimintoihin myös maamme rajojen ulkopuolelta.

Informaationsodankäynnin, kuten tietoverkkohyökkäysten, kohteina voivat olla päättäjät, kansalaiset, tiedotusvälineet, energialähteet, tietoverkot tai maanpuolustuksen keskeiset elementit kuten ilmapuolustus."

Selontekoon kirjatun Suomen turvallisuus- ja puolustuspoliittisen toimintalinjan mukaan sähköisten viestintä- ja tietojärjestelmien toiminnassa varmistetaan viestintäverkkojen ja niihin liittyvien järjestelyjen toimivuus ensisijaisesti kansallisesti, mutta myös kansainväliseen yhteistyöhön tukeutuen. Erityisesti varmistetaan valtiojohdon ja turvallisuusviranomaisten viestintä.

Hakkerointi tukee tulivoimaa

Suomen sotilaallisesta puolustamisesta selonteossa todetaan muun muassa, että tulivoiman merkitys säilyy keskeisenä ja myös ennaltaehkäisevänä tekijänä. Mutta samaan aikaan kaukovaikutteisten täsmäaseiden, elektronisen vaikuttamisen, satelliittiteknologian ja

informaatiosodankäynnin keinot ja merkitys lisääntyvät.

Myöhemmin todetaan myös, että:

"Puolustusvoimien integroiduilla tiedustelun, valvonnan ja johtamisen järjestelmillä tuotetaan tilannekuva maalta, mereltä, ilmasta sekä informaatio- ja tietojärjestelmäympäristöstä. Valtakunnallisesti keskitettyä järjestelmää hyödynnetään suunnittelun, johtamisen ja toimeenpanon nopeuttamiseksi.

Kykyä puolustautua vastustajan tietojärjestelmähyökkäyksiä vastaan ylläpidetään ja kehitetään. Koko yhteiskunnan voimavaroja hyödynnetään sotilaallisen puolustuksen tukemisessa maanlaajuisesti keskitetyillä logistiikkajärjestelmällä."

Tietoturva yhteiskunnan perusedellytys

Selonteon mukaan tietoturvallisuus on yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys. Sen haavoittuvimpia kohteita ovat avoimet tietoverkot.

"Sähköisten viestintä- ja tietojärjestelmien toiminta varmistetaan, jotta viranomaisten ja elinkeinoelämän toimintaan sekä kansalaisten turvallisuuteen kohdistuvat vakavat häiriötilanteet voidaan hallita.

Suomi kehittää sähköisten palvelujen ja tietoteknisen infrastruktuurin tietoturvallisuutta. Tietoverkkorikollisuuden torjunnassa tarvitaan reaaliaikaista yhteistyötä viranomaisten ja yksityisen sektorin välillä. Erityisen tärkeänä pidetään ennaltaehkäisevän toiminnan, toimijoiden roolien ja vastuiden jäsentämistä sekä tiedonvaihdon edistämistä."

Selonteko edellyttää, että viranomaisilla on käytössään nykYTEknologian tarjoamat varoitus- ja hälytysjärjestelmät, joiden avulla voidaan ehkäistä tai vähentää väestön turvallisuuteen ja yhteiskunnan toimivuuteen vaikuttavien äkillisten tapahtumien seurauksia.

Viranomaisradioverkon tulevaisuus turvataan riittävin voimavaroin, ja yhteiskunnan turvallisuudesta vastaavien viranomaisten viestiverkkojen yhteiskäyttöä edistetään.

Lisäksi viestintäalan keskeistä erityislainsäädäntöä tarkennetaan poikkeusolojen ja normaaliajan häiriötilanteiden varautumisvelvoitteiden osalta. Varautumisvelvoitteilla varmistetaan sähköisen viestinnän palveluiden toimivuus ja käytettävyys kaikissa olosuhteissa.

Oikea tilannekuva it:n avulla

Puolustusvoimien operatiivista johtamista kehitetään jatkamalla puolustusjärjestelmän tehokkaan käytön mahdollistavan johtamisjärjestelmän rakentamista. Integroitu tiedustelu-, valvonta- ja johtamisjärjestelmä tuottaa oikean tiedon tilannekuvan muodostamisen, suunnittelun, toimeenpanon ja vaikutusten seurannan toteuttamiseksi, selonteossa sanotaan.

Kehittämisen painopiste on yhteisen tilannetietoisuuden muodostamisessa ja varmennettujen tietoteknisten palveluiden kehittämisessä. Puolustusvoimien yhteinen johtamisjärjestelmä korvaa puolustushaarojen itsenäisiä järjestelmiä ja sovelluksia.

Kehittämisessä otetaan huomioon tietoverkkosodankäynti, ja puolustusvoimien johtamista tukevien järjestelmien kehittämisessä hyödynnetään korkeaa kansallista osaamista.

Kirjoittaja: Tuomas Linnake
tuomas.linnake@digitoday.fi

<http://www.itviikko.fi/tietoturva/2009/01/23/turvaselontekoverkkohyokkaykset-konkreettinen-uhka/20092049/7>