RO & PO/Soikkeli & Olin

Puolustusvaliokunta

Hybridiuhat ja kyberturvallisuus, informaatiopuolustus

1 Hybridivaikuttaminen

Hybridivaikuttamisella tarkoitetaan poliittisesti motivoitunutta suunnitelmallista toimintaa, jolla pyritään saavuttamaan omat tavoitteet erilaisia, toisiaan täydentäviä keinoja käyttäen ja kohteen heikkouksia hyödyntäen.

Hybridivaikuttamisen keinot voivat olla esimerkiksi taloudellisia, poliittisia, diplomaattisia tai sotilaallisia. Keinoja voidaan käyttää samanaikaisesti tai siten, että ne seuraavat toisiaan. Hybridivaikuttamista tehdään esimerkiksi informaatio-, kyber-, fyysisten ja taloudellisten operaatioiden avulla. Hybridivaikuttamisen takana voi olla joko valtiollinen tai ei-valtiollinen toimija. Valtiollinen taho voi käyttää ei-valtiollista tahoa, esimerkiksi rikollisryhmää, päämääränsä saavuttamiseen.

Puolustusselonteossa uhkakokonaisuutta lähestytään sotilaallisesta näkökulmasta laaja-alaisena vaikuttamisena. Laaja-alainen vaikuttaminen on sotilaallisessa varautumisessa käytettävä uhkakuva ja siihen kuuluu avoin sotilaallinen voimankäyttö osapuolten välillä.

Vaikuttamista voi olla vaikea tunnistaa, ja siinä hyödynnetään yhteiskunnan haavoittuvuuksia jo normaalioloissa. Vaikuttaja pyrkii itselleen edullisten olosuhteiden luomiseen ja omien päämääriensä edistämiseen käyttämällä keinoja, jotka soveltuvat parhaiten kuhunkin tilanteeseen. Tavoitteena on kohdevaltion puolustuskyvyn horjuttaminen esimerkiksi aiheuttamalla epävarmuutta väestön keskuudessa ja heikentämällä maanpuolustustahtoa ja valtion poliittisen johdon toimintakykyä.

2 Nykytila

Puolustusvoimat on kehittänyt kybertilannekuvan muodostamista, omien järjestelmien suojaamista ja valvontaa sekä puolustuksellisten kyberoperaatioiden suunnittelua ja toimeenpanoa. Kyberpuolustuksen integrointia osaksi operatiivista toimintaa on jatkettava ja se on sisällytettävä myös kaikkien eri toimialojen, viranomaisten ja muun yhteiskunnan väliseen tiiviiseen yhteistyöhön.

Informaatiopuolustuksen päämäärä on suojata maanpuolustuksen toimintoja ulkoa ohjatun ja muun vahingoittamistarkoituksessa tehdyn viestinnän vaikutuksilta. Informaatiopuolustus on osa koko yhteiskunnan suojautumista informaatiovaikuttamiselta. Informaation vahingoittava käyttö on jokapäiväinen osa laaja-alaista vaikuttamista. Puolustusvoimissa on kehitetty kykyä informaatioympäristön seurantaan, informaatiovaikuttamiselta suojautumiseen ja toimintaedellytysten luomiseen informaatioympäristössä. Informaatiopuolustuksesta on tullut osa Puolustusvoimien normaaliolojen toimintaa.

3 Kyber- ja informaatiopuolustuksen kehittäminen

Puolustushallinto varautuu laaja-alaiseen vaikuttamiseen yhdessä muiden toimijoiden kanssa osana kehittyvää kokonaisturvallisuuden mallia. Laaja-alaisen vaikuttamisen

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
kirjaamo@defmin.fi
www.defmin.fi

hallinta edellyttää usean hallinnonalan ennakointia ja varautumista sekä julkishallinnon kattavan yhteistyön syventämistä yksityisen sektorin, järjestöjen ja kansainvälisten kumppanien kanssa. Viranomaisyhteistyötä ja toimivaltuuksia, kyberpuolustuksen kansallista ja kansainvälistä yhteistyötä sekä strategista viestintää ja informaatiopuolustusta on kehitettävä edelleen vaikuttamiseen vastaamiseksi.

Puolustusjärjestelmän kybertilannekuvan parantaminen sekä kyberuhkien torjuminen edellyttävät tiedonvaihdon, toimivaltuuksien ja kansallisten yhteistyörakenteiden kehittämistä viranomaisten välillä. Viranomaisyhteistyön kehittämistarpeet on selvitettävä ja määriteltävä muutosten perusteiksi. Selvitystyön perusteella käynnistetään kyberpuolustuksen kehittämistoimenpiteet, mukaan lukien tarvittava säädösvalmistelu. Toimenpiteiden tavoitteena on varmistaa turvallisuusympäristön edellyttämät kyberpuolustuksen toimivaltuudet, osaaminen ja riittävät tiedonsaantioikeudet tilanne- ja valvontakuvan muodostamiseksi, suojautumisen toteuttamiseksi tarvittaessa aktiivisin vastatoimin sekä myös tarvittaessa vaikuttamiseksi vihamielisen toimijan kohdejärjestelmiin.

Liikenne- ja viestintäministeriön koordinoiman kyberturvallisuuden kehittämisohjelman mukaisesti viranomaisyhteistyön kehittämisen tarkastelu käynnistetään puolustusministeriön ja sisäministeriön yhteistyönä. Vastuista ja toimivaltuuksista johtuen on kuitenkin ilmeistä, että tarkasteluun liittyy myös valtiovarainministeriön hallinnonala, ulkoasiainhallinto sekä valtioneuvostotasoinen yhteistyö. Puolustusvoimien, Suojelupoliisin, poliisin, Kyberturvallisuuskeskuksen ja yhteisten palveluntuottajien yhteinen tilannekuva, operatiivinen yhteistyö, yhteiset toimintamallit ja niiden kehittäminen ovat keskeisessä roolissa.

Viranomaisten välistä yhteistyötä ja sen säädöspohjaa tarkasteltiin myös liikenne- ja viestintäministeriön johtamassa tietoturvallisuuden ja tietosuojan kehittämistä yhteiskunnan kriittisillä toimialoilla koskeneessa työssä, joka käynnistyi ns. Vastaamo-tapauksen jälkeen. Liikenne- ja viestintäministeriö on käynnistämässä sen osalta toimenpiteet, jotka otetaan huomioon tarvittavilta osin myös kyberpuolustuksen kehittämisessä.

Osaltaan kokonaisuuteen kuuluu myös valtiovarainministeriön johtama digitaalisen turvallisuuden kehittäminen, johon liittyy mm. tietojärjestelmien vaatimustenmukaisuutta ja sen arviointia koskeva lainsäädäntö. Kehittyvänä toimintona on myös verkkoturvallisuuden neuvottelukunta, joka perustettiin sähköisen viestinnän palvelulain ns. 5G pykälien mukaisesti varmistamaan kansallisen turvallisuuden ja maanpuolustuksen edut jatkuvasti kehittyvissä mobiiliverkoissa.

Kansainvälinen yhteistyö on keskeistä Suomen kyberturvallisuudelle ja kyberpuolustukselle. Suomen etu on tehdä tiivistä yhteistyötä kansainvälisten toimijoiden kanssa monenvälisesti, alueellisesti ja kahdenvälisesti. Tämä koskee niin teknistä yhteistyötä kuin poliittista vuoropuhelua.

Informaatiopuolustuksen merkitys on kasvanut edellisen selonteon jälkeen kyberuhkien torjuntakyvyn merkityksen tavoin. Ulkoa ohjatun ja muun vahingoittamistarkoituksessa jaetun informaation määrä ja levitystavat jatkavat lisääntymistään, ja tehokas informaatiopuolustus edellyttää Puolustusvoimilta mm. kehittyviä digitaalisia työkaluja informaatioympäristön seuraamiseksi ja puolustuksellisten toimenpiteiden käynnistämiseksi tarvittaessa. Informaatiopuolustuksessa ja informaatiovaikuttamiseen vastaamisessa on keskeistä kyetä yhteensovittamaan informaatiosisällöt ja viestinnän toimintatavat

viranomaisten ja muiden toimijoiden kesken vaikuttavan reagoinnin vaatimalla nopeudella. Informaatiopuolustuksen kykyjä kehitetään muiden viranomaisten ja kansainvälisten kumppanien kanssa varmistaen selkeät ja ajan tasalla olevat toimivaltuudet. Kehittämisessä otetaan huomioon muun valtiohallinnon informaatiovaikuttamiseen vastaamiseen liittyvät toimet.

Informaatiovaikuttamisen keinovalikoima on laaja. Vaikuttamista voidaan toteuttaa yhteiskunnallisin, poliittisin, viestinnällisin, psykologisin, sosiaalisin, taloudellisin ja sotilaallisin keinoin. Puolustusvoimien informaatiopuolustuksen on kyettävä havaitsemaan esimerkiksi laaja-alaiseen vaikuttamiseen liittyvä toiminta informaatioympäristössä ja tarpeellisilta osiltaan myös suojata oma toiminta. Informaatiopuolustusta kehitetään kouluttamalla omaa henkilöstöä, verkostoitumalla, tiedonvaihdolla, yhteisillä hankkeilla ja osallistumalla sekä kansallisiin että kansainvälisiin työryhmiin ja harjoituksiin. Informaatiopuolustuksen keskeinen perusta muodostuu tilannekuvasta, johon kootaan Puolustusvoimia ja sen toimintaa käsittelevät, eri medioissa ja alustoilla julkaistuun informaatioon liittyvät ilmiötasoiset tiedot. Tilannekuvan avulla luodaan edellytykset suojautumiselle ja operaatioiden tuelle, mihin liittyy läheisesti myös operaatioturvallisuus. Operaatioturvallisuudella tarkoitetaan omaan toimintaan liittyvän kriittisen tiedon tunnistamista ja suojaamista julkisen ja salassa pidettävän tiedon osalta. Tilannekuvan muodostamiseen liittyy keskeisesti toimivaltuudet, joihin perustuen viranomainen voi koota tietoa.

Kyber- ja informaatiopuolustuksen osalta keskeinen rooli on oman henkilöstön kouluttamisella sekä omien kyvykkyyksien kehittämisellä tutkimus-, kokeilu- ja kehittämistoiminnan avulla. Tähän pyritään vastaamaan mm. johtamisjärjestelmäkoululla, jonka toiminta kyber- ja informaatiopuolustuksen osaamiskeskuksena on käynnistymässä vuoden 2022 alusta. Koulun tehtävänä on palkatun henkilöstön ja asevelvollisten koulutuksen lisäksi edistää mm. digitalisaatiota ja innovointia sekä yhteensovittaa johtamisjärjestelmiä, kyber- ja informaatiopuolustusta sekä elektronista sodankäyntiä. Tuoreen päätöksen mukaisesti aikaisemmin melko pienimuotoisesti toteutettu kybervarusmiesten koulutus laajenee koulun perustamisen myötä.

4 Yleisesti resurssitarpeista

Puolustusvoimien yhteisten ja Maa-, Meri- ja Ilmavoimien suorituskykyjen kehittämisen ohella lisäresursseja tarvitaan uusiin teknologioihin liittyvään osaamiseen, kyber-, avaruus- ja informaatiosuorituskykyjen kehittämiseen sekä sotilastiedustelulainsäädännön toimeenpanoon. Tässä muistiossa tarkasteltujen osa-alueiden osalta tarpeet tarkentuvat suunnittelun edetessä ja selontekoa toimeenpantaessa. Resurssitarpeisiin voivat vaikuttaa myös muualla yhteiskunnassa kehitettävät kyvykkyydet.

Puolustushallinnossa on jo pitkään tunnistettu tarve lisätä Puolustusvoimien henkilöstömäärää noin 600 henkilötyövuodella. Näistä noin 100 toteutuu kuluvalla vaalikaudella. Tavoitteena on kasvattaa henkilöstömäärää 500 henkilötyövuodella asteittain 2020-luvun loppuun mennessä niin, että se vastaa velvoitteiden edellyttämää tarvetta. Jotta varusmiesten kouluttajamäärätavoite, 2,5 kouluttajaa/joukkue, voidaan saavuttaa, sopimussotilaiden määrä on turvattava 350 henkilötyövuoden tasolle.

Henkilöstön asteittainen lisääminen edellyttää resurssien lisäämistä. Henkilöstömäärän kasvattaminen 500 henkilötyövuodella edellyttää tavoitetilassaan 2020-luvun loppuun mennessä noin 38 milj. euron vuosittaista pysyvää tasokorotusta. Sopimussotilaiden 350 henkilötyövuoden tason turvaaminen tarkoittaa vuosittain 80 henkilötyövuoden lisäystä