



RO/ Tuomo Rusila
Vanhempi osastoesiupseeri, everstiluutnantti

7.10.2024

FI.PLM.
Asianumero

Puolustusvaliokunta

Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko kyberpuolustuksen näkökulmasta

Puolustusvaliokunta on pyytänyt puolustusministeriön asiantuntijalausuntoa Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteon käsittelyä varten. Tässä puolustusministeriön lausunnossa käsitellään selontekoa kyberpuolustuksen ja sen kehittämisen näkökulmasta.

Petteri Orpon hallitusohjelman mukaan hallitus laatii kyberpuolustuskoktiinin sekä selkeyttää ja tarkentaa Puolustusvoimien roolia kyberpuolustuksessa. Valtioneuvoston ulko- ja turvallisuuspoliittisen selonteon toimintaympäristökuvaus sekä kyberdiplomatiaa, -puolustusta, -turvallisuutta ja -rikostorjuntaa käsittelevät painopisteet ja tavoitteet tukevat kyberpuolustukselle hallitusohjelmassa asetettuja päämääriä. Lisäksi ne antavat perusteita niin kansallisen kyberturvallisuusstrategian kuin puolustusselonteon kyberpuolustusta käsittelevien osioiden laatimiseksi.

1 Ulko- ja turvallisuuspoliittisen selonteon keskeiset kirjaukset kyberpuolustuksen toimeenpanon näkökulmasta

Kyberpuolustuksen näkökulmasta Valtioneuvoston ulko- ja turvallisuuspoliittisen selonteon kirjaukset voi ryhmitellä neljään kokonaisuuteen. Ensimmäisessä kokonaisuudessa selonteko käsittelee toimintaympäristön ja teknologian muutosta sekä näiden seurauksia. Toisessa kokonaisuudessa käsitellään Suomen turvaamista ja vihamieliseen toimintaan vastaamista. Kolmantena kokonaisuutena voidaan nähdä kansallisen kyberpolitiikan kehittäminen. Kansainvälinen yhteistyö sekä integroituminen Naton kyberpuolustukseen muodostavat neljännen kokonaisuuden. Kyberpuolustuksen kehittämisen näkökulmasta osiot muodostavat eheän ja loogisen kokonaisuuden.

Teknologinen murros yhdessä digitaalisesta toimintaympäristöstä entistä riippuvaisemman yhteiskunnan kanssa muodostavat aikaisempaa otollisemman ympäristön valtiolisten päämäärien ajamiseen myös vihamielisin keinoin. Samalla niin siviiliyhteiskunnan tuen kuin kybertoimintaympäristön luomien mahdollisuuksien merkitys on kasvanut maanpuolustukselle ja sotilasoperaatioiden toteuttamiselle. Vihamielinen kybertoiminta on vakiintunut osaksi voimapolitiikkaa ja valtiollisen vaikuttamisen keinovalikoimaa. Näitä tukevia kyber- kuin informaatio-operaatioita toteutetaan jatkuvasti myös normaalioloissa. Vaikuttamisessa pyritään pidättäytymään aseellisen voimankäytön kynnyksen alapuolella. Tämä hämärtää sodan ja rauhan rajaa sekä haastaa eri toimijoiden nykyisiä rooleja, toimivaltaa ja lähestymistapaa kyberuhkiin. Tietoturva- ja resilienssilähtöinen lähestyminen ei muuttuneessa toimintaympäristössä yksin riitä kansallisten intressien ja toimintavapauden suojaamiseksi. Myöskään pyrkimykset valtiollisten toimijoiden saattamiseen rikosvastuuseen eivät välttämättä ole tehokkaimpia tapoja vastata rikollisesta toimintalogiikasta poikkeavaan pahantahtoiseen toimintaan.

Koska digitaalisen ympäristön merkitys yhteiskunnan normaalille toiminnalle on kasvanut, on samalla lisääntynyt sen tärkeys myös valtiolliselle suvereniteetille ja sen turvaamiselle. Valtioneuvoston ulko- ja turvallisuuspoliittisen selonteon todennäköisesti laajakantoisin ja periaatteellisin kyberympäristöön liittyvä tavoitteenasettelu liittyy juuri tähän. Valtiollisen suvereniteetin turvaamista kybertoimintaympäristössä ei ole aikaisemmin asetettu näin selvästi kansalliseksi tavoitteeksi. Suvereniteetin turvaamisen



7.10.2024

FI.PLM.
Asianumero

RO/ Tuomo Rusila
Vanhempi osastoesiupseeri, everstiluutnantti

keskeisinä painopisteinä voidaan selonteon mukaan nähdä kansallista päätöksentekoa, viranomaistoimintaa, kriittistä infrastruktuuria ja puolustusjärjestelmää vastaan toteutettujen vakavien kyberhyökkäyksien ennalta estäminen ja torjunta, olivat tekijöinä sitten valtiolliset tai niiden lukuun toimivat tahot. Uhkien ennaltaestämistä ja torjuntaa tukevat niin kansallinen kyky attribuoida vihamieliseen kybertoimintaan syyllistyneet tahot kuin toteuttaa riittäviä ja oikea-aikaisia vastatoimia. Vastatoimien toteuttamiseksi tulee kyetä hyödyntämään käytössä oleva koko keinovalikoima. Näihin tavoitteisiin pääsemistä tukee tiivistyvä sotilas-siviiliyhteistoiminta sekä yksityisen sektorin kanssa tehtävä läheinen yhteistyö. Turvaamalla valtiollinen suvereniteettimme myös kyberympäristössä vahvistetaan sääntöpohjaista valtioiden välistä toimintaa, puolustuksen pelotevaikutusta sekä tuetaan ulko-, turvallisuus- ja puolustuspoliittisten päämäärien saavuttamista. Kybertoimintaympäristön merkityksen kasvu edellyttää myös näiden päämäärien saavuttamista tukevan kansallisen kyberpolitiikan tarkentamista.

Kansallista kybertoimintaa ei voida tehdä ilman kansainvälistä yhteistyötä. Kyberpuolustuksen näkökulmasta keskeistä ovat integroituminen Naton kyberpuolustukseen, EU:n ja Naton yhteistyön tiivistäminen, EU:n valmiuksien ja suorituskykyjen kehittäminen, sekä kahden ja -monen välinen yhteistyö liittolaisten ja kumppanien kanssa. Naton kyberpuolustus on parhaillaan muutoksessa ja sitä kehitetään tukemaan entistä paremmin liittokunnan pelotetta ja puolustusta. Pääosa Naton kybersuorituskyvyistä on jäsenvaltioiden kyvykkyyksiä, joilla mahdollistetaan liittokunnan missioiden ja operaatioiden toteuttaminen rauhan, kriisin sekä konfliktin aikana ja joilla tarvittaessa kyetään tukemaan liittolaisia näiden kyberkriiseissä. Kahdenvälisellä kyberpuolustuksen yhteistyöllä kehitetään halutuilla osa-alueilla yhteistä operointi- ja suorituskykyjä molempia hyödyttävässä laajuudessa.

2 Ulko- ja turvallisuuspoliittisen selonteon painopisteet ja tavoitteet kyberpuolustuksen kehittämisen näkökulmasta

Valtioneuvoston ulko- ja turvallisuuspoliittisen selonteon mukaan kyberpuolustusta tulee kehittää osana Suomen kokonaisturvallisuutta ulko-, turvallisuus- ja puolustuspoliittisten tavoitteiden mukaisesti. Keskeinen osa tämän tavoitteen saavuttamista on kansallisen kyberpuolustusdoktriinin luominen. Valmistuttuaan se kuvaa, miten Suomi vastaa vihamieliseen valtiolliseen kybertoimintaan hyödyntäen kaikkia kansallisia voimavaroja ja keinoja. Lisäksi doktriini kuvaa kybertoimintaympäristön valtiollisen suvereniteetin turvaamisen periaatteet. Doktriinissa huomioidaan kansainvälisten toimijoiden, tärkeimpinä EU, Nato ja keskeiset liittolaiset, kyvykkyyksien hyödyntäminen kansallisen kyberpuolustuksen tukena, mutta myös se miten Suomi voi tukea muita.

Kyberpuolustusdoktriini tullaan valmistelemaan poikkihallinnollisesti puolustusministeriön johdolla. Doktriinin laatiminen edellyttää perusteita niin ulko- ja turvallisuuspoliittisesta selonteosta, puolustusselonteosta ja kyberturvallisuusstrategiasta, mutta myös muuta työn aikaista ohjausta. Ulko- ja turvallisuuspoliittisen selonteon kuvaamat painopisteet ja tavoitteet antavat osaltaan hyvät perusteet doktriinityön käynnistämiseksi.

Valmisteilla oleva kansallinen kyberturvallisuusstrategia kuvaa laaja-alaisesti tavoitteita ja kehittämistehtäviä, joilla tuetaan myös kyberpuolustuksen kehittämistä. Strategiassa kyberpuolustusta käsitellään kahdella tasolla, kansallisella ja sotilaallisella, jotka kytkeytyvät kansalliseen kyberturvallisuuteen. Kansallinen kyberpuolustus käsittää ne kansalliset ja kansainväliset sotilaalliset ja siviilialojen toimet, joilla turvataan Suomen valtiollinen itsenäisyys sekä kansan elinmahdollisuudet ja turvallisuus ulkoisia, valtioiden



7.10.2024

FI.PLM.
Asianumero

RO/ Tuomo Rusila

Vanhempi osastoesiupseeri, everstiluutnantti

aiheuttamia kyberuhkia- ja häiriöitä vastaan sekä toimeenpannaan tarvittavat vastatoimet kaikissa valmiustiloissa. Sotilaallinen kyberpuolustus vuorostaan kattaa ne toimet, joilla turvataan Suomen puolustuskykyyn vaikuttavat järjestelmät ja eri sektorien toimijat erityisesti valtiollisilta uhkatoimijoilta ja niiden edustajilta puolustuskyvyn varmistamiseksi sekä turvataan Suomen suvereniteettia ja toimeenpannaan sotilaalliset kyberoperaatiot. Kansallisen kyberpuolustuksen taso muodostaa kyberpuolustuskoktriini pääkäsitteilytason.

Puolustusvoimien roolin tarkentaminen ja selkeyttäminen kyberpuolustuksessa tulee edellyttämään Puolustusvoimien tehtävän ja toimivaltuuksien päivittämistä lainsäädännössä. Kehitystarpeet on tunnistettu Puolustusvoimien strategisen suunnittelun osana, vuonna 2022 valmistuneessa puolustushallinnon omassa selvitystyössä sekä vuonna 2023 valmistuneessa poikkihallinnollisessa virkamiesmietinnössä. Keskeisimmät säädöspohjan kehitystarpeet ovat kyberpuolustuksen määrittäminen Puolustusvoimien tehtäväksi, erilaiset tiedonvaihdon ja tiedonhankinnan kehittämistarpeet sekä virka-avun ja viranomaisten yhteistoiminnan kehittäminen. Lisäksi tarpeen on tarkentaa kyberoperaatioiden ja erityisesti kybervaikuttamisen toimivaltapohjaa aseellisen hyökkäyksen kynnyksen alapuolisessa toiminnassa, muun muassa vastatessa vihamieliseen valtiolliseen kybetoimintaan. Kansainvälisen avun antamista ja vastaanottamista koskevan lainsäädännön päivittäminen on keskeistä myös kyberpuolustuksen kansallisille ja kahdenvälisille toimintamahdollisuuksille, mutta myös täyspainoisen osallistumisen mahdollistamiseksi Naton puolustukseen ja pelotteeseen. Valtioneuvoston ulko- ja turvallisuuspoliittisesta selonteosta suoraan johtuva säädöspohjan kehittämistehtävä on kyberympäristön suvereniteetin valvonnan ja turvaamisen toteuttamisen toimivalta. Tarve käynnistää kyberpuolustuksen lainsäädäntöhanke tuotaneen esille myös valmisteilla olevassa puolustusselonteossa.

Liitteet

Jakelu PLM Kansliapäällikkö
PLM RO OSPÄÄL
PLM PO OSPÄÄL
PLM erityisavustajat
PLM sotilasneuvonantaja

Tiedoksi PLM ROTI Tietohallintojohtaja