TkT Catharina Candolin
Kyberturvallisuuden erityisasiantuntija
2.5.2022

Lausunto sotateknologian tulevaisuudesta ja sen vaikutuksesta Suomen turvallisuuteen

Eduskunnan tulevaisuusvaliokunta on pyytänyt asiantuntijalausuntoa sotateknologian tulevaisuudesta ja sen vaikutuksesta Suomen turvallisuuteen. Keskityn lausunnossani kyberpuolustukseen liittyvän sotateknologian kehittymiseen ja sen vaikutuksiin. Teknologian osalta ei ole tarkoituksenmukaista erotella sota- ja siviiliteknologia, sillä nämä ovat pitkälti samoja. Lisäksi kyberpuolustus on aiheena laaja, eikä teknologian kehitys riitä kuvaamaan sen tulevaisuutta ja vaikutusta.

Kyberpuolustus koostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Tiedustelu tarkoittaa tässä viitekehyksessä tietojen keräämistä toisen valtion tietojärjestelmistä ja -verkoista sekä laitteista, jotta niihin voidaan myöhemmin tarvittaessa vaikuttaa esimerkiksi muuttamalla, häiritsemällä tai tuhoamalla niiden toimintaa. Suojautuminen puolestaan tarkoittaa toisen valtion suorittaman tiedustelun ja vaikuttamisen ennaltaehkäisemistä, estämistä ja torjumista. Kybertiedustelun ja -vaikuttamisen kohteet eivät rajoitu valtion asevoimiin, vaan kattavat käytännössä koko yhteiskunnan. Erityisesti kriittinen infrastruktuuri on mahdolliselle vihamieliselle toiminnalle houkutteleva kohde, sillä yhteiskunnan toiminta on siitä riippuvainen.

Kyberpuolustukseen liittyvät menetelmät ovat jatkuvassa kehityksessä rinnakkain yleisen teknologiakehityksen kanssa. Uusi teknologia voi olla sekä kybervaikuttamisen kohteena, että sen mahdollistajana. Keskeisiä kehitysalueita ovat muun muassa tekoäly ja koneoppiminen sekä kvanttitietokoneet ja kryptologia. Uuden teknologian lisäksi vanhaa teknologiaa jää edelleen käyttöön, jonka takia kybertiedustelu ja -vaikuttaminen eivät välttämättä edellytä uusien menetelmien kehittämistä, vaan olemassa olevien menetelmien soveltamista.

Tekoäly ja koneoppiminen: Tekoälyä ja koneoppimista tullaan soveltamaan myös kyberoperaatioissa. Odotusarvona on, että tekoälyn ratkaisuilla kyetään toteuttamaan hyvin kohdennettuja ja erikoistuneita kyberhyökkäyksiä nopeasti ja laaja-alaisesti, samalla välttäen kohteen havainnointi- ja suojaustoimenpiteitä. Toisaalta tekoälyä ja koneoppimista hyödynnetään enenevissä määrin myös suojausratkaisuissa. Lisäksi tekoälyratkaisut voivat olla kybervaikuttamisen kohteena, jolloin vihamielinen taho pyrkii esimerkiksi huijaamaan tekoälyn toimimaan haluamallaan tavalla. Esimerkiksi syöttämällä tekoälyn algoritmeille väärennettyä dataa, voidaan vaikuttaa tekoälyn ja siten kohteiden toimintaan.

Kvanttitietokone ja kryptologia: Ensimmäiset kvanttitietokoneiden prototyypit on jo rakennettu ja on arvioitu, että kvanttilaskennan hyödyt alkavat näkyä laajasti yhteiskunnassa ja ihmisten arjessa jo 2030-luvulla. Yksi mahdollinen soveltamisala kvanttilaskennalle on nykyisten salausratkaisuiden purkaminen. Tämä tarkoittaa sitä,

että valtion, yritysten, organisaatioiden ja yksityishenkilöiden tiedot jäävät vaille salausratkaisuiden tarjoamaa suojaa ja voivat paljastua ulkopuolisille, tai niitä voidaan oikeudettomasti muuttaa ilman, että sitä havaitaan. On olemassa riski, että salattua tietoa kerätään talteen jo nyt ja puretaan myöhemmin, kun kvanttitietokoneet ovat kehittyneet riittävän tehokkaiksi. Myös kryptovaluutat arvioidaan olevan murrettavissa tulevaisuudessa kvanttilaskennan avulla. Kvanttiturvallisia ratkaisuja kehitetään jatkuvasti, mutta työ perinteisten ratkaisuiden korvaamiseksi pitäisi aloittaa jo nyt.

Vanhat teknologiat sovellettuna uudella tavalla: Kehitys ei rajoitu pelkästään uuteen teknologiaan ja sen hyödyntämiseen, vaan myös olemassa olevia ratkaisuja voidaan käyttää uudella tavalla. Esimerkiksi niin kutsutut ransomware -hyökkäykset ovat yhdistäneet haittaohjelmat ja salausteknologiat siten, että kohteeksi joutuneiden tiedot salataan, jonka jälkeen kohteelta on vaadittu rahaa salauksen purkamisesta. Sekä haittaohjelmat että salausratkaisut ovat ”vanhaa teknologiaa”, mutta niitä on viime vuosina sovellettu laajamittaisesti vihamieliseen toimintaan aiheuttaen valtaisia taloudellisia menetyksiä kohteille. Tulevaisuudessa on siis ennustettavissa, että myös nykyisiä teknologiaratkaisuja sovelletaan uusilla tavoilla.

Teknologiakehityksestä huolimatta on syytä huomioida, että yhteiskunnan eri toimijoilla on edelleen käytössä paljon vanhaa teknologiaa, josta on vaikeata päästä nopeasti eroon. Myös nykyaikainen teknologia saattaa olla haavoittuvainen ja siten altis hyväksikäytölle. Lisäksi teknologian kehittyminen tuo mukanaan uusia tietoturvahaasteita.

> Esimerkiksi 5G ei ole, toisin kuin aikaisemmat sukupolvet, pelkästään lisää verkkokapasiteettia tuottava tiedonsiirtoratkaisu, vaan tuo mukanaan myös uusia toimintamalleja. Puhutaan jopa paradigmamuutoksesta. Monet sovellusalueet tulevat ottamaan harppauksen 5G:n myötä. Esimerkiksi esineiden internet (Internet of Things, IoT) tulee mullistumaan kiitos mahdollisuuden liittää paljon laitteita verkkoon sekä tuoda tietojenkäsittelyominaisuuksia lähelle verkon reunaa, itseohjautuvat autot voivat kommunikoida keskenään ja sopia liikennöinnistä paikallisesti, terveydenhuolto kykenee hyödyntämään fyysiseen sijaintiin perustuvia ratkaisuja, jne. Tietoturvallisuutta on 5G:n osalta mietitty enemmän kuin aikaisempien sukupolvien kohdalla ja 5G-standardi määritteleekin joukon parannuksia viestinnän ja käyttäjien tietoturvallisuuden ja tietosuojan parantamiseksi. Tosin mitään kokonaistietoturva-arkkitehtuuria ei ole määritelty. Haasteita on kuitenkin lukuisia; muun muassa verkon ytimen ja reunan välinen ero hämärtyy, virtualisointi tuo omia haasteitaan verrattuna fyysisesti eristettyihin ympäristöihin ja matalan suojaustason laitteiden määrä lisääntyy. Näin ollen suojattava pinta-ala kasvaa, mutta on epäselvää, miten eri tietoturvaratkaisuja sovelletaan ja ylläpidetään käytännössä.

Riskienhallinta tulee olemaan nykyistä haasteellisempaa. Teknisten haasteiden lisäksi 5G:n ympärillä velloo isompi, poliittinen kysymys. Samaan aikaan kuin valtioiden kyky toimia kyberympäristössä kehittyy, herää kysymys valtioiden mahdollisesta vaikuttamisesta laitetoimittajiin.

Kyberpuolustuksen suorituskykyjen kehittäminen ei kuitenkaan ole pelkästään teknologiakehittämistä, vaan myös johtamisjärjestelmän, osaamisen, menetelmien ja toimintatapojen kehittämistä.

Merkitykset Suomen turvallisuudelle ovat seuraavat:

Suomen suvereniteetin puolustaminen myös kyberavaruudessa: Suomi voi joutua laajamittaisen kyberhyökkäyksen kohteeksi. Laajamittainen hyökkäys saattaa kohdistua esimerkiksi kriittiseen infrastruktuuriin, samalla väliaikaisesti lamauttaen koko Suomen. Jos kyberhyökkäys on vaikutuksiltaan ja laajuudeltaan rinnastettavissa aseelliseen hyökkäykseen, on Suomella oikeus puolustautua. Tämä edellyttää, että Suomella on:

- Attribuutiokykyä: sekä teknistä kykyä että poliittista tahtoa tunnistaa tekijä ja tuoda asia julki.
- Kyky ja valmius vastatoimiin: Suomella tulee olla käsitys millaisiin vastatoimiin Suomi voisi ryhtyä. Vastatoimet eivät rajoitu toimintaan kyberavaruudessa.
- Laaja kansallinen kybertilannekuva: Tilannekuva, joka kattaa niin viranomaiset kuin yksityisen sektorin soveltuvin osin, esimerkiksi kriittisen infrastruktuurin.
- Operatiiviset johtosuhteet tulee olla määriteltyjä ja toiminta on harjoiteltava, jotta tositilanteessa kyetään toimimaan tarkoituksenmukaisesti.
- Kansainväliset verkostot, joiden kanssa olla yhteistoiminnassa tarvittaessa.
- Lainsäädäntö, joka antaa viranomaisille tarvittavan mandaatin toimia.

Suomessa olevat toimijat ovat kybertiedustelun (ja myöhemmin vaikuttamisen) kohteena: Suomessa olevat toimijat (organisaatiot ja ihmiset) ovat innokkaita ottamaan uutta teknologiaa käyttöön. Teknologia on läpitunkevaa; sitä puetaan päälle, siinä asutaan (älykodit), sen kanssa leikitään ja viihdytään (lasten lelut, viihdelaitteet), sen kanssa seurataan ja kehitetään terveyttä (älykellot ja sormukset), se vastaa elintoiminnoistamme (sydäntahdistimet), se tukee päivittäisiä toimintoja (maksuliikenne, terveydenhuolto, yhteydenpito), jne. Teknologiatoimittajiin ja -ratkaisuihin ei tosin aina ole luottamista. Tämä avaa mahdollisuuksia vieraiden valtioiden kohdistamalle tiedustelulle (sekä vaikuttamiselle).

Suomessa on teknologiaosaamista: Suomessa on teknologiaosaamista, myös kyberpuolustuksen ja -turvallisuuden alalla. Lisäksi Suomessa on osaamista mitä tulee tekoälyyn sekä kvanttiteknologiaan ja -salaukseen. Tämä osaltaan vaikuttaa Suomen turvallisuuteen myönteisesti, varsinkin jos tätä teknologiaosaamista halutaan kehittää. Lisäksi kyber- ja teknologiateollisuutemme voisi olla vahvempi vientituote, jolla voisimme osaltamme olla mukana vahvistamassa koko Euroopan turvallisuutta.

Kyberammattilaisten riittämättömyys: Sekä Suomessa että muualla maailmassa on pula kyberalan asiantuntijoista. Tämä liittyy sekä teknologiaosaamiseen, että kyberalan osaamiseen laajemmin. Jos emme kykene kouluttamaan ja houkuttelemaan riittävää osaamista Suomeen syntyy riski, että putoamme kelkasta kyberpuolustuksen ja -turvallisuuden osalta.

Suomen kyberpuolustuksen kehittämisen mahdollisuudet: Puolustusvoimat vastaa Suomen kyberpuolustuskyvyn kehittämisestä, kattaen tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyt. Tämä edellyttää erityisesti panostusta osaamisen kehittämiseen sekä puolustusvoimissa että yksityisellä sektorilla. Panostamalla Suomen omaan kyberpuolustukseen vahvistamme nykyistä kansallista maanpuolustusta myös kyberavaruuden osalta. Tässä on tosin syytä ottaa huomioon, että suojautuminen tässä viitekehyksessä ja tällä hetkellä tarkoittaa vain puolustusvoimien oman toiminnan suojaamista toisen valtion tiedustelulta ja vaikuttamiselta. Se ei siis yksinään vastaa Suomen suvereniteetin puolustamiseen kyberavaruudessa samalla tavalla kuin maalla, merellä ja ilmassa.

Kybertiedustelu ja -vaikuttaminen sekä siitä suojautuminen on jatkuvaa kehitystä sekä teknologian että menetelmien osalta. Turvallisuutta ei rakenneta keskittymällä pelkästään teknologiaan, vaan ymmärtämällä aiheen kokonaisuutta ja monimuotoisuutta. Teknologioita tulee ja menee, mutta toiminnan luonne pysyy ennallaan; valtiot pyrkivät edistämään omia poliittisia, taloudellisia ja sotilaallisia tavoitteitaan, niin kyberavaruudessa kuin muualla.