Lausunto
17.4.2018

Puolustusvaliokunta

KYBERUHKIEN KEHITYS JA KASVAVA MERKITYS TIEDUSTELULAINSÄÄDÄNNÖSSÄ

Kansallisella kyberkyvykkyydellä on tulevaisuudessa yhä keskeisempi merkitys kokonaisturvallisuuden ja yhteiskunnan elintärkeiden toimintojen turvaamisen sekä Suomen kilpailukyvyn kannalta. Suomi on yksi maailman digitalisoituneimmista yhteiskunnista.

Turvallisuus on yhteiskuntamme kivijalka, ja samalla yhä vahvempi kilpailuetumme kansainvälisesti. On huomioitava, että elämme turvallisuusympäristössä, jota leimaavat muutosnopeus, ennalta-arvaamaton epävakaus ja kompleksisuus. Lisäksi teknologia ja digitalisaatio ulottuvat hiljalleen kaikille elämänalueille. Olemme riippuvaisempia ja toisaalta myös haavoittuvaisempia digitaalisen toimintaympäristön toimivuudesta – sekä luotettavuudesta ja turvallisuudesta – kuin koskaan aikaisemmin. Tulevaisuuden kehitys näyttää tältä osin vääjäämättömältä: Digitaalinen toimintaympäristö muodostuu yhä hallitsevammaksi ja strategisemmaksi läpi globaalin toimintakentän.

Suomi tarvitsee toimivan lainsäädännön, jotta tiedustelukykymme olisi nykytarpeita vastaava. Tilanneymmärryksen ja -kuvan merkitys turvallisuudessa korostuu, ja tämä on yksi keskeinen syy tiedustelulainsäädännölle.

Huolehtiaksemme Suomen turvallisuudesta, on sen tapahduttava kaikissa toimintaympäristöissä: maalla, merellä, ilmassa ja myös kybertoimintaympäristössä. Sanoisin, että turvallisuusviranomaisemme eivät suorita tehtäviään hyvin, jolleivat he ole kykeneviä huolehtimaan turvallisuudessa näissä kaikissa toimintaympäristöissä. Nyt käsiteltävässä lainsäädännössä on kyse lainsäädännön sopeuttamisesta muuttuvaan digitalisoituvaan toimintaympäristöön. Tällä hetkellä lainsäädäntömme ei ota huomioon kybertoimintaympäristön erityispiirteitä. Lisäksi viimeaikainen huolestuttava kehitys Suomen turvallisuusympäristössä korostaa tarvetta luoda nopealla aikajänteellä säädöstöä ja menetelmiä, joilla parannetaan kyberuhkiin liittyvää torjunta- ja ennakointikykyä. Reaaliaikaisen kybertilannekuvan muodostaminen ja jaetun tilannetietoisuuden aikaansaaminen tulee puolestaan olla nykyisessä turvallisuusympäristössä yhä nopeampaa.

On hyvä, että Suomeen luodaan selkeä ja avoin säädöspohja tiedustelulle. Tiedustelulle on tarpeen sopia selkeät pelisäännöt, jotta voimme luottaa sen hoitamiseen asiallisesti ja yhteiskunnan kannalta kestävällä tavalla. On hyvä, että Suomessa olemme valinneet tien, jossa myös yksityisyydensuojaan ja perusoikeuksiin sekä lainsäädännön valvontaan liittyviä kysymyksiä on pohdittu tarkasti.

Tarkoin on myös arvioitava minkälaisia velvoitteita lainsäädäntö aiheuttaa muille yhteiskunnan toimijoille, kuten yrityksille. Kohtuuttomiin tai epäselviin velvoitteisiin liittyisi elinkeinopoliittisia riskejä. Tiedustelu on alue, jota tulee säännellä selkeästi epävarmuuksien ja -selvyyksien välttämiseksi myös investointinäkökulmasta. Nyt esitellyt lakiehdotukset ovat kieltämättä hyvin laaja kokonaisuus, johon perehtyminen vie paljon aikaa, eikä aihepiiri yksityiskohtineen ole kovin helppo ymmärtää. Lainsäädäntö on myös ehdotuksissa hajautunut useiksi laiksi, jolloin kokonaisuus voi jäädä epäselväksi.

Kyberuhkien nykytila ja kehitys

Kyberuhkat ovat muuttuneet vaikutuksiltaan aiempaa moninaisemmiksi ja haitallisemmiksi niin yksittäisille ihmisille, yrityksille kuin suomalaiselle yhteiskunnalle. Kuten fyysisessä maailmassa, niin myös kybertoimintaympäristössä on useita eri motiiveilla toimivia toimijoita. Kehittyneimmät toimijat ovat valtioita, joille kybertoimintaympäristö on strateginen ympäristö. Esimerkiksi tiedon digitalisoitumisen myötä on luonnollista, että myös valtioiden välinen vakoilu on siirtynyt yhä enemmän digitaaliseen maailmaan. Digitaalisen toimintaympäristön kehitykseen yhdistyy yhä merkittävämmällä tavalla valtioiden halu luoda erilaisia kyberkyvykkyyksiä. Tietyssä määrin voidaan sanoa, että maailmassa on parhaillaan käynnissä globaali kyberasevarustelukilpa. Kyse on kehityssuunnasta, jossa valtiot resursoivat kasvavissa määrin erilaisten kyberkyvykkyyksien kehittämisen, mihin liittyy yhä keskeisemmin halu ja kyky hankkia kybertoimintaympäristöä kautta tietoa valtiollisiin tarkoituksiin. Kuvaavaa nykyhetken tilanteesta on Yhdysvaltojen uhkakuvien priorisointi, jossa tämän maailman luultavasti teknologisesti kehittynein valtio nostaa kyberuhkat sekä kybervakoilun vakavimmaksi kansallista turvallisuuttaan uhkaaviksi tekijöiksi.

Kyberoperaatioilla on nykyisin erottamaton sijansa missä tahansa modernissa sodassa, konfliktissa ja kriisissä. Esimerkiksi edelleen jatkuvassa Ukrainan sodassa näkyvimpiä kyberaktiviteetteja ovat olleet muun muassa ukrainalaisiin televisiokanaviin, lehdistöön ja Naton verkkosivuihin kohdistuneet palvelunestohyökkäykset, valtiollisten organisaatioiden ja poliittisten päättäjien viestiyhteyksien häirintä, internetissä olevan tiedon ja videoiden manipuloiminen, presidentinvaalien aikana keskusvaalilautakunnan tietojärjestelmiin murtautuminen, luottamukselliseksi luokiteltujen sähköpostien, puheluiden ja asiakirjojen vuotaminen julkisuuteen sekä erilaiset tietoverkkojen ja -järjestelmien toimintahäiriöt. Teknologisesti kehittyneet valtiot kykenevät käymään sotaa tänä päivänä fyysisen maailman rinnalla myös digitaalisessa ympäristössä, johon moderni yhteiskuntarakenne tarjoaa uusia sodankäynnin tapoja – ja haavoittuvuuksia.

Kybersodankäynnissä ja -vaikuttamisessa ollaan niin kykyjen luomisessa kuin niiden käyttämisessä siirtymässä kehittyneempään vaiheeseen. Suurvallat ovat rinnastaneet kyberhyökkäykset sotilaallisiin toimiin, joihin voidaan vastata kaikin mahdollisin keinoin. Viime vuosien aikana on voitu havaita kyberhyökkäyksissä yhä systemaattisempaa toimintatapaa ja hyvää toiminnan organisointia ja johtamista. Hyökkäysmenetelmät ovat yhä kehittyneempiä ja käytetyt ”kyberaseet” yhä tehokkaampia. Ennusteiden mukaan myös

valtioiden kybersodankäynnin kyvykkyydet tulevat edelleen kehittymään sekä hyökkäysten laajuudessa että kehittyneisyydessä. Valtioiden tekemät kyberhyökkäykset tulevat vaikuttamaan poliittisiin suhteisiin sekä valtarakennelmiin ympäri maailmaa. Valtioiden käyttämät työkalut valuvat sitten jollakin aikavälillä myös kyberrikollisryhmien käyttöön.

Erilaisia vakoiluhaittaohjelmia on viime vuosina löytynyt maailmalta lisääntyvissä määrin, mutta todellinen kysymys kuitenkin lienee, että mitä kaikkea tietoverkoissa ja -järjestelmissä liikkuu, joista emme edes ole tietoisia. Havainnointikyky ja sen kehittäminen on keskeisimpiä kyberturvallisuuden kehitysalueita, jotta voimme parantaa turvallisuuttamme. Meillä ei ole nyt riittävää havainnointikykyä siitä, mitä julkisen ja yksityisen sektorin verkoissa tapahtuu ja miksi. Suomessa on tähän mennessä havaittu yksi vakava tunkeutuminen. Tapauksia on varmasti enemmän, mutta niitä ei ole joko ole kyetty havainnoimaan tai niistä ei ole raportoitu julkisesti.

Kohdistetuissa hyökkäyksissä hyökkääjä hyödyntää aktiivisesti löydettyjä kohdeorganisaation palvelujen haavoittuvuuksia ja heikkouksia. Kohdistetut hyökkäykset ovat yleensä ammattimaisesti toteutettuja ja niihin on yleensä varattu osaavat ja hyvät resurssit. Hyökkäykset kohdistetaan kansallisiin salaisuuksiin, aineettomiin pääomiin sekä henkilötietoihin. Hyökkäykset saatetaan toteuttaa pitkän aikavälin kuluessa. Hyökkäyksiä voidaan muuntaa, sovitella sekä kehittää, jotta voidaan hyödyntää kohdeorganisaation heikkouksia mahdollisimman hyvin. Kohdistetut hyökkäykset toteutetaan usein kampanjoina, jolloin ne koostuvat sarjasta epäonnistuneita ja onnistuneita yrityksiä päästä syvemmälle ja syvemmälle kohdeorganisaation verkkoon. Yleensä ne kohdistuvat tiettyihin toimialoihin ja hyökkääjillä on pitkän tähtäimen päämäärä mielessä. Kohdistetuissa hyökkäyksissä hyödynnetään useita erilaisia tekniikoita, esimerkiksi drive-by lataukset, haittaohjelmat, vakoiluohjelmat, tietojenkalastelu sekä roskapostit. Jatkuvien kohdistettujen hyökkäysten takana on usein jokin valtiollinen toimija tai valtion kanssa hyvin läheisesti toimiva rikollisryhmä. Kohdistetuissa hyökkäyksissä hyödynnetään usein ns. nollapäivähaavoittuvuuksia ja nk. watering hole -hyökkäyksiä. Ne ovat hakkereille erityisen arvokkaita. Hakkerit pitävät yleensä hyvin salassa löytämänsä nollapäivähaavoittuvuudet, jotta niitä voisi hyödyntää mahdollisimman pitkään. Watering Hole -hyökkäykset tehdään yleensä saastuneilla web-sivustoilla; ne aktivoituvat vasta kun vierailija tulee tietystä IP-osoitteesta. Tämä piilottaa hyökkäyksen hyvin. Jopa tietoturvatutkijoilla on haasteellista löytää watering hole -haittaohjelma, koska he tulevat web-sivulle eri IP-osoitteesta. Kun tällainen hyökkäys löydetään, siirtyvät hyökkääjät toiselle sivustolle käyttäen taas jotakin muuta löydettyä nollapäivä-haavoittuvuutta.

Rahan motivoimat rikolliset ovat siirtyneet sinne missä rahat ovat – digitaaliseen maailmaan. Kyberrikoksista on tullut mustilla markkinoilla toimiva vahva ja elinvoimainen liiketoiminnan alue. Kehityssuuntana on kyberrikollisuuden ammattimaistuminen, kansainvälistyminen ja käytettyjen menetelmien kehittyminen. Kyberrikollisuus on tällä hetkellä nopeimmin kasvava rikollisuuden laji, jonka arvioidaan maksavan yhteiskunnille maailmanlaajuisesti yli 400 miljardia dollaria vuosittain. Teollisuusvakoilu tunkeutuu organisaatioiden ytimiin digitaalisen maailman kautta samalla, kun perinteiset rikokset,

kuten valelaskutus ja muut huijaukset, ovat löytäneet uusia väyliä sähköistyneistä taloushallintajärjestelmistä ja sähköpostista.

Yksi kasvava joukko digitaalisessa toimintaympäristössä on tietoverkoissa toimivat aktivistit, haktivistit, joiden motiivina on mielen osoittaminen. Kyse on eri muodoin ja usein varsin impulsiivisesti tapahtuvasta protestoinnista. Uudemmilla haktivisti-ryhmillä on kykyä vaativampiinkin vaikuttamiskeinoihin digitaalisessa ympäristössä. Haktivismi tulee toisaalta ymmärtää yleisemmin yhteiskunnalliseen vaikuttamiseen osallistumisena, johon digitaalinen maailma antaa uudenlaisia mahdollisuuksia. Mutta silloin kun tehdään laittomuuksia aktivismin nimissä, on se tuomittavaa yhtä lailla fyysisessä maailmassa kuin digitaalisessa ympäristössä. Esimerkiksi kybervandalismi ja laiton hakkerointi ovat yhä useammin poliisien rikostutkinnan kohteena. Kyse on usein tekijänsä mielestä harmittomasta toiminnasta, mutta näytönhalusta tehty palvelunestohyökkäys on rikos, jonka vahingot voivat olla suuria ja josta voi saada vankeutta.

Erityistä huolta on viime aikoina aiheuttanut ääriryhmien ja terroristien kykyjen kehittyminen digitaalisessa toimintaympäristössä. Esimerkiksi ISIS on tehokkaasti hyödyntänyt eri digitaalisia kanavia propagandansa levittämisessä, rekrytoinnissa, rahaliikenteensä hoitamisessa sekä keskinäisessä viestinnässä. Ääriryhmien motiivi luoda pelkoa ja tehdä järjettömiltä tuntuvia iskuja on saanut monet pohtimaan, että olisiko ISIS:llä lähivuosina kykyä tehdä digitaalisen maailman kautta iskuja, joilla olisi ihmishenkiä uhkaavia vaikutuksia fyysisessä maailmassa. Erityisesti Yhdysvalloissa ja Iso-Britanniassa on arvioitu ISIS:n pyrkivän kyberhyökkäyksillä vaikuttamaan kriittisen infrastruktuurin, kuten vesi- ja voimalaitoksien, toimintaan.

Kyberympäristön turvallisuus kilpailuetuna

Kybertoimintaympäristöä ei tule nähdä vain uhkina vaan myös voimavarana ja mahdollisuutena Suomelle. Suomella on osaavana ja yhteistyökykyisenä maana erinomaiset edellytykset nousta yhdeksi kyberturvallisuuden kärkimaaksi maailmassa. Meillä on vahva osaamisperusta sekä pitkät perinteet tiivistä yksityisen ja julkisen sektorin yhteistyöstä sekä hallinnon alojenvälisestä yhteistyöstä. Kyberturvallinen toimintaympäristö parantaa myös Suomen houkuttelevuutta investointikohteena. Näiden lisäksi kyberturvallisuus on itsessään kasvava liiketoiminnan alue. Kyberturvallisuuden osaamistamme ja ratkaisujamme arvostetaan maailmalla. Samalla digitaalisen turvallisuuden yhteydessä keskustellaan kansainvälisesti yhä enemmän luottamuksesta, mikä on turvallisuuden kolikon toinen puoli. Ilman luottamusta ei voi rakentaa turvallisuutta. Suomella on vahva kansainvälinen luottamuspääoma hyödynnettävänään. Selkeä tiedustelulainsäädäntö sekä Suomen kyky huolehtia turvallisuudestaan myös kybertoimintaympäristössä osaltaan vahvistavat entisestään suomalaista luottamuspääomaa.

Aalto-yliopisto

Professori Jarno Limnéll