Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

9.8.2024

Liikenne- ja viestintäministeriö

Viite: VN/36693/2023

Lausunto: Suomen kyberturvallisuusstrategia

Teknologiateollisuus ja Kyberala kiittävät mahdollisuudesta lausua asiasta. Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Teknologiateollisuuden yritykset tuottavat puolet Suomen viennistä ja tutkimus- ja kehitysinvestoinneista sekä työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Huoltovarmuusorganisaation digipooli yhtyy lausuntoon.

Lausunnon tiivistelmä

Suomen kyberturvallisuusstrategia on tärkeä asiakirja ei pelkästään EU-oikeuden vaatimusten näkökulmasta, vaan myös siksi, että sillä voidaan suunnata politiikkatoimia, hallinnon ja eri toimijoiden yhteistyön kehittämistä sekä julkisten varojen huolellista ja vaikuttavaa käyttöä. Julkisen hallinnon sitoutuminen kyberturvallisuuden kehittämiseen on välttämätöntä yhteiskuntamme digitaalisen turvallisuuden edistämiselle.

Valtion periaatepäätöksenä annettavan kyberturvallisuusstrategian tavoitteena on uudistaa strategia vastaamaan muuttunutta toimintaympäristöä ja hallitusohjelman kirjauksia sekä täyttää NIS2-direktiivin asettamat vaatimukset.

Vaikka elämme geopoliittisten muutosten aikaa ja perinteiset sodan ja asevoiman uhat ovat nousseet, kyberturvallisuusstrategian tärkein tehtävä on luoda suuntaviivoja ja edellytyksiä päivittäisen elämän eli hallinnon, talouden ja kansalaisyhteiskunnan digitaalisten riskien hallinnalle. Tämä on myös NIS2-direktiivin ydin. Hallitusohjelman mukaan hyvinvoinnin perusta on kestävä talous. Suomen hyvinvoinnin rahoitus onnistuu rakentamalla vahvuuksiemme pohjalta kilpailukykyistä ja yritysmyönteistä Suomea, joka vahvistaa luottamusta oikeusvaltioon, houkuttelee investointeja ja rohkaisee taloudelliseen toimeliaisuuteen. Yhteiskunnasta välittäminen edellyttää Suomea, jonka kilpailukyvyllä ja kasvulla hyvinvointi voidaan rahoittaa.

Strategialuonnos jättää kuitenkin osin vaikutelman, että tarkoitus on listata, mitä viranomaiset haluaisivat itse tehdä ja mitä resursseja niihin haluttaisiin. On laajasti tiedossa ja kiistatonta, että Suomen talous, niin yksityinen kuin julkinen on merkittävissä vaikeuksissa eikä kestävyysvajeeseen ole odotettavissa parannusta lyhyellä aikavälillä. Kuluvalla vuosikymmenellä nähtäneen jatkuvaa julkisen talouden välttämättömiä sopeutustoimia. Tämä ei kuitenkaan vaikuta ohjaavan keskeisiä suuntaviivoja, vaikka tarve on pakottava ja poliittinen ohjaus on olemassa. Tästä syystä kaksi tavoitetta tulisi nostaa kaikkein keskeisimmiksi:

1. Kaikkien toimialojen yritysten tukeminen kyberturvallisuuden riskienhallintakeinojen käyttöönotossa.
2. Suomessa toimivan kyberturvallisuusteollisuuden elinvoiman tukeminen, myös osaamisen kehittämisen osalta. Osana muita teknologia- ja vientiyhtiöitä kyberturvallisuusalan yhtiöt tuottavat sekä ratkaisut kaikkien toimijoiden kyberturvallisuuden hallintaan, että verotuloja, joilla viranomaisten omia toiveita voidaan kestävästi rahoittaa.

Teknologiateollisuus ry
Kyberala ry

Eteläranta 10, P.O.Box 10, FI-00131 Helsinki
Telephone +358 9 192 31
www.techind.fi
Business ID: 0215289-2

Neljästätoista kehittämisehdotuksesta vain kahdessa (ekosysteemin kehittäminen ja kvanttilaskennan uhat) kehittäminen ulottuu keskeisiltä osin viranomaistoiminnan ulkopuolelle. Strategian tavoitetilan hahmottelu on näkemyksellinen, mutta temaattisesti kolme pääelementtiä eli yhteistyö ja koordinointi, teknologinen kehitys sekä osaaminen eivät jäsennä toimenpiteitä ja toimijuutta riittävästi:

- Yhteistyön ja koordinoinnin tulisi perustua ajatukseen siitä, miten julkinen sektori voi tukea Suomessa sijaitsevia organisaatioita kyberturvallisuuden riskienhallintakeinojen toimeenpanossa – myös taloudellisesti – sekä tukeakseen niitä tarjoavien yritysten elinvoimaisuutta.
- Teknologinen kehitys tulee nähdä osana edellä olevaa, eikä erillisenä ”varautumistoimena”. Tällöin keskiössä ovat strategian teollisuuspoliittiset painotukset sekä edellisessä kohdassa mainittu digitaalisten riskien hallinta (vähintään yhteiskunnan keskeisten toimijoiden osalta).
- Osaamis- ja osaajapulan ratkaiseminen ei riitä, sillä ilman taloudellisen kasvun verotuottoja julkinen sektori ei pysty hyödyntämään osaajia. Yritysten osalta osaajia palkataan vain, mikäli kysyntää on olemassa ja kasvun mahdollisuuksia näköpiirissä.

Strategian osa-alueet (pilarit) kuvaavat pikemminkin mahdollistajia (enabler), kuin varsinaisia strategian osa-alueita. Katsomme, että visiossa tulisi näkyä selkeästi, miten nyt tunnistetut ongelmat on ratkaistu vuonna 2035. Näin vision mukaisen tilan saavuttaminen olisi merkittävämpää, erillisten kehitystoimien tekemisen sijaan.

Seuraavassa esitetään tarkemmat huomiot liittyen strategialuonnoksen yksittäisiin lukuihin.

Toimintaympäristön muutos

Vaikka kyberturvallisuudella varmistetaankin osaltaan kansallisen turvallisuuden, maanpuolustuksen, huoltovarmuuden, elinkeinoelämän ja kansalaisyhteiskunnan toimintaedellytykset voitaneen silti todeta, että Suomen (taloudellista) hyvinvointia ei voida perustaa varautumisajatukseen aseellisesta uhkasta tai poikkeusoloista. Digitaalisen resilienssin tärkein elementti on päivittäinen jatkuvuus eli yhteiskunnan toimijoiden käyttämien viestintä- ja tietojärjestelmien (ml. data) ylläpitämien tietovirtojen ja palveluiden luottamuksellisuus, eheys ja saatavuus. Jokaisella, joka hallitsee edellä mainittuja, on oma vastuunsa ja roolinsa toteuttaa soveltuvia riskienhallintatoimia (esim. vahva osapuolten tunnistautuminen ja tarkka pääsynvalvonta sekä kvanttiturvalliset eri käyttötapauksille agnostiset verkkoyhteydet).

Tästä näkökulmasta strategian tavoitetilan ilmaisua ”Suomi havaitsee, tunnistaa, torjuu ja kestää kyberhäiriötilanteita, toipuu niistä sekä toimii päättäväisesti vastatessaan häiriöihin.” tulisikin mukauttaa vastaamaan monitoimijuuden todellisuutta: ”Suomessa havaitaan, tunnistetaan, torjutaan…”. Suomi-termillä saatetaan ymmärtää virheellisesti valtiokäsitettä ja siten viitattavan yksinomaan valtion viranomaisten toimintaan.

Samassa yhteydessä voitaneen myös perustellusti kysyä, mitkä ovat ne perusteet ja keinot, joiden avulla ”päättäväisyys” osoitetaan? Tarkoitetaanko päättäväisyydellä julkisia taloudellisia panostuksia, poliittista huomiota vaiko kenties laittomasti toimivien valtioiden vastuuseen saattamista esim. pakotteiden tai muiden diplomaattisten keinojen avulla?

Toimintaympäristön kuvaus osio vaikuttaa pyrkivän ylläpitämään terminologian avulla hallinnonalojen intressejä ja -työnjakoa, osin perustellusti, mutta samalla myös osin oikeusvaltion näkökulmasta virheellisesti. Tällainen lähestymistapa edistää heikosti niitä tavoitteita, joita strategialle on ehdotettu. Tiivistäen: käytännössä kaikki tietoturvaloukkaukset täyttävät jonkin

rikoksen tunnusmerkistön. Se, että vain murto-osasta tietoturvaloukkauksia kirjataan rikosilmoitus, ei muuta tätä tosiasiaa. Näin ollen katsomme, että strategiassa jonkinlaiseen tahallisuusoppiin perustuville määritteille ”pahantahtoinen” tai ”vihamielinen” ei tässä yhteydessä ole tarvetta.

Koska jokaisella viestintä- ja tietojärjestelmien haltijalla on vastuu omaisuudestaan ja siten myös siihen kohdistuvien rikosriskien hallinnasta, organisaatioiden toimintaroolin ”supistaminen” vastuuseen lähinnä ”ohjelmiston päivittämisessä” on virheellinen. Vastaavasti epämääräisiksi ja määrittelemättömiksi jätettyjen ”NATOn (liittokunnan) suorituskyvyt”, ”infrastruktuuri”, ”seitsemän resilienssin perusvaatimukset” jättävät näiden kirjausten tosiasiallisen vaikutuksen laittoman vahingollisen toiminnan vähentämiseksi arvailujen varaan. Strategian ymmärtämisen kannalta olisi hyödyllistä todeta, että myös kyberpuolustus nojaa pääosin omaisuuden ja toimintakyvyn suojaamistoimiin. ”Hyökkäykset” ymv. termit olisi perusteltua varata ainoastaan tarkoituksiin, jossa laiton toiminta olisi jo lähtökohtaisesti katsottavissa väkivaltaiseksi (aseelliseksi) toiminnaksi Suomen alueellista koskemattomuutta tai poliittista riippumattomuutta vastaan (esim. sivu 18). Asiaa on osin käsitelty ansiokkaasti Nykytila-luvussa (s. 19.).

Kuten yltä ilmenee, useat terminologiset valinnat ohjaavat strategian sisältöä. Asiakirjan lopusta löytyvän termien kuvauksen osalta on syytä nostaa esille, että koko strategiadokumenttia ja sen vaikuttavuutta voi merkittävästi heikentää sellainen termien valinta ja määrittely, joita ei ole valmisteltu laajasti eri intressitahojen kanssa tai muutoin hyväksyttävällä tavalla (olemassa oleva terminologinen viitekehys). Koska alan terminologia on monelta osin vakiintumatonta ja koska tarkoituksena on laatia laajasti vaikuttava pitkän ajan strategia, on tarpeen, että käytettävien merkityksellisten ja täsmällisten termien tulee olla laajasti ja yleisesti niitä soveltavien tahojen yhteistyössä hyväksyttyjä. Luonnosversio jättää vaikutelman, että termien määrittely on tehty kevyesti ja sidosryhmiä osallistamatta. Tämä ilmenee osin myös terminologian epätarkkuudesta, tarkoitushakuisuudesta sekä virheellisyydestä.

Katsomme, että myös kokonaisturvallisuuden näkökulmasta Suomen ehdottomasti tärkein viitekehys on Euroopan Unioni ja asia tulisi ilmaista selkeästi strategiassa (esim. sivu 12). Asian suhteen olisi perusteltua tunnistaa, että myös kyberturvallisuuden edistämisessä taloudellisen ja normatiivisen (ml. diplomatia) vallan osalta Euroopan Unioni on keskeisin toimija.

Lisäksi on perusteltua todeta, että sekä kansallisesti että EU:n tasolla sääntely ja sen vaatimat investoinnit eivät välttämättä aiheuta haittoja suurille taloudellisille toimijoille, mutta hankaloittaa EU:n alueelle sijoittautuneiden PK-sektorin toimijoiden kasvua. Kolmansien maiden toimijat voivat kasvaa sääntelyn ulkopuolella ja vallata EU:n sisämarkkinoita kasvunsa turvin. Näillä toimijoilla ei ole kannustimia toteuttaa Suomen, tai muunkaan pienen jäsenvaltion kansallisia vaatimuksia. EU:n sisäinen kilpailu, kansallisten vaatimusten fragmentaatio ja protektionismi asettavat haasteita kehitykselle suhteessa Unionin ulkopuolisiin valtioihin. Tästä näkökulmasta on hyvin perusteltua, että kansallisia vaatimuksia harmonisoidaan EU:n yhteisellä sääntelyllä.

Kansallisen toimintamallin kehittämisen osalta voisi olla hyödyllistä selkeyttää, että kyberturvallisuusalan varautumisen ja yhteistyön avulla tavoitteena on tukea kaikkien alojen kyberturvallisuuden kehittymistä toimialan palvelutuotannon avulla (s.13).

Toimintaympäristön muutosta (s. 11) ja nykytilaa (s. 16) koskevista luvuista tulisi siirtää tavoitteita tai päämääriä koskevat ilmaisut tavoitteita koskeviin lukuihin. Esimerkiksi:

- ”Kyberturvallisuuteen ja -puolustukseen liittyvät kansalliset EU- ja Nato-kannat on tärkeää sovittaa yhteen.” (s. 13).
- ” Lainsäädännön, viranomaisten toimivaltuuksien ja yhteistyörakenteiden ja -verkostojen kehittäminen onkin välttämätöntä.” (s. 14)

Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

Yhteenveto:
- Monitoimijuuden merkitystä tulisi korostaa käyttämällä ”Suomi”-termin sijasta ”Suomessa”.
- Epämääräisten ja määrittelemättömien termien käyttöä tulisi välttää, tai määritellä kansallista vuoropuhelua edistävällä tavalla.
- Selvennetään termin ”päättäväisyys” perusteet ja keinot kyberuhkiin vastaamisessa.
- Euroopan Unionin merkitystä Suomen tärkeimpänä viitekehyksenä tulisi korostaa.

Nykytila

Suomen kyberturvallisuusstrategian tavoitetila ulottuu vuoteen 2035 ja se ottaa huomioon murrosteknologioiden vaikutuksen kyberturvallisuuteen. Kvanttiteknologian huomioonottamista on korostettu, luultavimmin osin sen pitkäkestoisuudenkin vuoksi, mutta kuitenkin mm. tekoälyn käsittely on jätetty vähemmälle. Joka tapauksessa tutkimuslaitosten, korkeakoulujen, elinkeinoelämän ja julkishallinnon tulee toimia riittävän ketterästi muuttuvassa teknologiakentässä.

Yhteenveto:
- Panostetaan kyberturvallisuuden koulutukseen ja jatkuvaan oppimiseen.
- Luodaan kansallinen kyberturvallisuusosaamisen ja -koulutuksen kehys.

Tavoitetila ja rakenne, sekä pilarit

Jotta strategian pohjalta voidaan tehdä toimintasuunnitelma, on tärkeää, että strategiaan kirjatut päämäärät ja tavoitteet ovat selkeitä ja yksiselitteisiä. Kun tavoitteita on paljon kasvaa houkutus yhdistellä asioita samoihin otsikoihin, mutta tämä näennäinen tavoitteiden lukumäärän pieneneminen ei todellisuudessa vähennä tavoitteiden määrää, mutta tekee niistä epämääräisempiä ja vaikeammin hyödynnettäviä toteutussuunnitelman pohjana.

Pilareita (osa-alueita) ja niiden strategisia tavoitteita koskevissa luvuissa on epäselvää, mitkä sisällöt vastaavat mitäkin strategista tavoitetta. Esimerkiksi innovatiivinen ja kokeileva kyberekosysteemi alaotsikko esiintyy kahteen kertaan, eikä ole selvää, mihin strategiseen tavoitteeseen otsikoiden alaiset tekstit liittyvät.

Yhteenveto:
- Erotellaan selkeästi erilliset tavoitteet omiksi kohdikseen (koskee sekä päämääriä, että eri osa-alueiden strategisia tavoitteita)
- Valitaan käyttöön joko termi “osa-alue” tai “pilari”, mutta ei molempia
- Nimetään osa-alueet yhdellä selkeällä otsikolla kahden tason sijaan, esimerkiksi: “Kansallinen ja kansainvälinen yhteistoiminta” ja “Uhkiin reagointi ja vastatoimet”
- Kirjoitetaan tavoitetila ja rakenne lukuun auki tavoitetilan erilliset päämäärät, jotka on nyt vain yhdellä lauseella ilmaistu luvun alussa olevassa laatikossa.
- Pilareita ja niiden strategisia tavoitteita koskevissa luvuissa tulisi alaotsikoinnin vastata luvun alussa olevassa laatikossa esitettyjä strategisia tavoitteita.

I Osaaminen, teknologia ja tutkimus-, kehitys- ja innovaatiotoiminta (TKI)

Kyberturvallisuusstrategiassa tulisi kuvata tarkemmin, miten tieto- ja teknologiapolitiikan tasonnostoa sekä uuden digitaalisen pehmeän infrastruktuurin kehittämistä sekä teknologian nopeampaa hyödyntämistä ja innovaatioiden skaalaamista tavoitellaan. Näitä keinoja ovat mm. yritysvetoisen TKI-yhteistyön lisääminen korkeakoulujen kanssa sekä TKI-toimintaan tarvittavan infrastruktuurin kehittäminen (mm. suurteholaskenta, kvanttilaskentapalvelut, datan saatavuuden parantaminen, kehittämisyhteistyö viranomaisten kanssa yhdessä sekä salausteknologian sertifioinnin tutkimuslaboratorio).

Kvanttilaskennan aiheuttamiin uhkiin varautumisen lisäksi kvanttilaskennan positiiviset vaikutukset kyberturvallisuuteen tulee hyödyntää, ja tämä tulisi myös ilmaista strategiassa. Suomi on kvanttiteknologioissa useita verrokkimaita edellä etenkin kvanttitietokonelaitteistojen osalta. Suomella on vahva kilpailuasetelma erityisesti raudankehityksessä ja suprajohtavissa teknologioissa. Myös hallitusohjelmassa panostetaan Suomen kvanttikyvykkyyden kehittämiseen. Kyberturvallisuuden varmistaminen tulevaisuudessa edellyttää yhtäältä omavaraisuuden saavuttamista kvanttilaskentateknologioissa ja toisaalta aktiivista kansainvälistä yhteistyötä sekä osaamisen kehittämistä.

Lisäksi (s. 17) Nykytila-luvun kirjaukseen "*Salausteknologioiden viranomaisarviointien ja -hyväksyntöjen hitaus ja kansallisen salausteknologisen laboratorion puuttuminen voivat pahimmillaan estää kehitystyötä*." ei liity kehitysehdotuksia sivulla 25, tai muuallakaan. Todettu puute tulisi huomioida kehitysehdotuksissa havaittavasti.

Tietoturvallisuustuotteiden arviointien ja hyväksyntöjen hitaus on jo estänyt ja hidastanut tuotteiden viemistä markkinoille. Hyväksyntöjen toteutus on hidasta ja kustannusintensiivistä teknologian kehittäjälle. Vastuussa olevien viranomaisten lain tulkinnat ovat olleet vaikeasti ennakoitavia ja osin kyseenalaisia, mikä on lisännyt kustannuksia ja viiveitä. Julkisen sektorin hankkija usein vaatii, että tuote on sertifioitu, mutta valvovalla viranomaisella ei ole resursseja tai velvollisuutta arviointiin/sertifiointiin. Valvovan viranomaisen tulisi luoda tehokkaat prosessit, joka mahdollistavat ja edesauttavat kansallisten ratkaisujen markkinoille saattamista.

Strategian mukaan kyberturvallisuuden tutkimus-, kehitys- ja innovaatiotoiminnassa hyödynnetään EU:n ja NATOn tarjoamat kansainväliset yhteistyö- ja rahoitusmahdollisuudet ja panostetaan niissä tarvittaviin prosesseihin, resursseihin ja ennakoivaan yhteistyöhön. Tähän panostaminen on perusteltua, jotta Suomi voisi menestyä EU:n, NATO:n ja EDA:n hankkeissa, mutta kuten edellä on todettu kansallinen TKI-toiminta ei voi perustua vain kansainväliseen kilpailtuun rahoitukseen.

Tavoitteen saavuttamiseksi tarvittaisiin myös kansallinen rahoitusratkaisu. Yhdeksi pilari I:n strategiseksi tavoitteeksi tulisi harkita kansallisen kyberturvallisuuden TKI-ohjelman perustamista tai olemassa olevan ohjelmien (Business Finland Digital Resilience -ohjelma ja/tai Traficomin Kyberturvallisuuskeskuksen Kansallinen koordinointikeskus NCC-FI) kehittämistä vahvemmin tähän suuntaan. Ohjelman tulisi toimia ainakin vastinrahoitusmekanismina kv-instrumenttien täydeksi hyödyntämiseksi sekä mahdollisesti myös hallitusohjelmassa jo sovitun kansallisen yhteiskehitysbudjetin osana yksinomaan rahoitetuille toimille. Ohjelma tulisi toteuttaa TK(I)-rahoituslain määrittelemän TK(I)-lisärahoituksen sisällä. Ohjelmassa tulisi korostaa yritysvetoisuutta ja yhteistyötä yritysten ja yliopistojen välillä. Rahoituksen kohdistaminen tulisi toteuttaa kilpailtuna rahoituksena. Tämän lisäksi ohjelmassa kannattaisi hyödyntää yliopistoille ja tutkimuslaitoksille varattua EU-vastinrahoitusta. EU:n TKI-instrumenttien tehokkaampaan käyttöasteeseen tulee tähdätä, mutta pullonkaulana on muun muassa yrityskonsortioiden luominen. Suomen tulee käynnistää TKI-vienninedistämisen toimet myös kyberturvallisuuden alueella, joissa keskitytään EU:n TKI-rahoitukseen parempaan saantoon kyberturvallisuuden osalta.

Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

Pilarin III:n TKI-toiminnassa tarvitaan proaktiivista työskentelyä, jotta Suomi voisi menestyä kansainvälisissä rahoitushauissa. Tämä edellyttää, että TKI-toimijat ja rahoitustoimijat osallistuvat entistä vaikuttavammin kansainväliseen kyberturvallisuuden ohjelmatyöhön, jotta tuleviin rahoitusohjelmiin saataisiin mukaan kansallisen kyberresilienssin kehittämistä tukevia sisältöjä. Rahoitusohjelmiin vaikuttaminen tulisi nostaa osaksi kansallista strategiaa.

Kyberturvallisuuden osaamisen ja koulutuksen osalta strategia nostaa hyvin esiin alan koulutuksen ja harjoitustoiminnan merkityksen koko TKI-toimintakentässä. Kohdassa ”Osaaminen on kaikilla tasoilla vahvaa” (s. 23) edellyttää lisäresursseja kyberturvallisuuden tutkintokoulutukseen, jatkuvaan oppimiseen sekä muunto- ja täydennyskoulutuksiin korkeakouluissa. Kansallisen kyberturvallisuusosaamisen vahvistamiseksi tulisi laatia osana tämän strategian toimeenpanoa laaja-alainen kyberturvallisuusosaamis- ja koulutusohjelma, jossa osaamistarpeet on katettu monipuolisesti. Strategiassa tulisi kuitenkin tehdä selkeämpi ero kyberturvallisuusalan ammattiosaamisen ja ns. laajojen kansanosien kyberriskitietoisuuden (kansalaistaitojen) välille, sillä kyberturvallisuusalan tuotannon ja viennin kasvu sekä organisaatioiden riskienhallinnan kehittäminen ovat riippuvaisia osaavan työvoiman saatavuudesta. Kilpailukyvyn edistämisessä yritysten lisäksi toimintaan osallistuvat korkeakoulut ja tutkimuslaitokset, jolloin myös kotimainen kyberturvallisuusalan TKI-toiminta on keskeistä kyberturvallisuuden ekosysteemin kehittämiseksi ja ylläpitämiseksi. Niin julkisella sektorilla kuin yksityisellä sektorillakin tarvitaan lisää osaamista ja todellisia mahdollisuuksia, suunnitella ja toteuttaa modernia, vaikuttavaa kyberturvallisuutta. Tämä aspekti olisi hyvä olla näkyvästi myös rakenteen kaavakuvassa.

Kyberharjoitustoiminnan tulisi kattaa laajasti kriittisen infrastruktuurin toimijoiden lisäksi julkishallinto ja yrityssektori sekä kansainväliset kumppanit. Lisäksi kansalaisille tarvitaan mahdollisuuksia harjoitteluun, jota voivat erityisesti tarjota alan yritykset. Kyberharjoitusympäristöjä ja -toimintamalleja on kehitettävä vastaamaan toimintaympäristön muutosta. Toimintaa tulisi tukea julkisin varoin. Tavoitteena tulisi olla, että harjoitustoiminnalla kehitetään koko yhteiskunnan kykyä torjua tietoturvaloukkauksia ja niiden haitallisia vaikutuksia.

Sivulla 22 sinisen laatikon 3. kohtaan tulisi lisätä termi ohjelmistot seuraavasti: ”*Suomi ottaa etulinjassa käyttöön murrosteknologioiden hyödyt ja edellyttää laitteisiin, ohjelmistoihin ja palveluihin sisäänrakennettua turvallisuutta*.”

Yhteenveto:

- Tieto- ja teknologiapolitiikan tasonnostoa ja digitaalisen infrastruktuurin kehittämistä tulisi kuvata tarkemmin.
- Tunnustetaan tietoturvallisuuden tuotteiden arviointi-/sertifiointitoiminnan puutteellisuuden aiheuttamat vahingot alan toimijoille ja Suomen taloudelle.
- Salausteknologian hyväksynnän viranomaispalvelu tulisi käsitellä kehitysehdotuksissa.
- EU ja NATO yhteistyö- ja rahoitusmahdollisuuksien hyödyntäminen tulisi varmista kansallisen TKI-vastinrahoitusinstrumentin avulla.
- Kyberturvallisuusalan ammattiosaaminen ja kansalaisten kyberturvallisuustietoisuus tulisi erottaa selkeämmin toisistaan.
- Kyberturvallisuusosaamisen tutkintojen tuottamisen tavoitteet ja pääkeinot tulisi kuvata tarkemmin osana koko teknologia- ja ICT-alan koulutustavoitteita.
- Kyberharjoitustoiminnan kehittämisen tavoitteet tulisi kuvata tarkemmin.

II Varautuminen

Vaikka digitaalinen toimintaympäristö sisältää uudehkoja uhkia yhteiskunnan toimivuudelle ja ns. matalatasoisen, mutta huomattavan vahinkovaikutuksen sisältävä toiminta on aiempaa helpompaa, perusratkaisut ovat edelleen haitallisten seurausten ennalta estäminen eli soveltuvien riskinhallintakeinojen käyttöönottaminen mahdollisimman laajasti yhteiskunnassa – ei yksinomaan keskeisten toimijoiden piirissä. Suomessa on esimerkiksi n. 78 000 työnantajayritystä ja 370 000 yrittäjää. Jokainen näistä on osa taloudellisen toimeentulon jatkuvuutta, tuottaen n. 60% Suomen bruttokansantuotteesta. Monitahoisiin uhkiin vastaamiseksi kansallisen ”varautumismallin” tulisikin kannustaa soveltuvien riskienhallintakeinojen käyttöönottamiseen ja kehittämiseen.

Tästä näkökulmasta koko yhteiskunnan varautumisen haaste onkin se, että monien toimialojen kyberkypsyyttä rajoittaa yritysten omat resurssit. Tarvittavia resursseja eli osaamista ja omaa pääomaa ei ole riittävästi käytettävissä. Mikäli siis strateginen tavoite on yhteiskunnan kyberturvallisuusriskien pienentäminen, tulee taloudellista tukea ohjata yrityksille niin, että ne kykenevät toteuttamaan soveltuvia riskienhallintatoimia. Nykyinen varautumisen malli on auttanut pitkälti riskienhallintatarpeiden tunnistamisessa, mutta toistuvat selvitykset ovat osoittaneet, että kehitystä ei kuitenkaan tapahdu yhteiskunnan kannalta riittävän nopeasti ja riittävissä määrin. Tämä on pitkälti liiketoiminnan realiteeteista johtuva haaste. On sekä kallista, että epätarkoituksenmukaista, että haastetta yritetään ratkaista viranomaisten resursseja lisäämällä.

Varautuminen on resurssi-intensiivistä. Varautumisen ytimessä on ajatus, että henkilötyötä ohjataan miettimään ja toteuttamaan järjestelyjä etukäteen sen suhteen, mikä voi mennä pieleen, miten tilanteesta voitaisiin palautua ja etenkin, mitä investointeja mahdollisesti tarvitaan toimintakyvyn turvaamiseksi. Siksi varautumisen kehittämisen tulisi keskittyä resurssienkäytön optimointimahdollisuuksiin ja tällaista toimintaa tukevaan rahoitukseen (esim. tarpeelliset muutokset Digitaalinen turvallisuus 2030-ohjelmaan). Teknologian kehittyessä ja uudistuessa varautumisen kyvykkyyttä tulisi upottaa eri toimintojen operatiivisiin toteutuksiin sen sijaan, että tehdään erillisiä varautumiseen liittyviä ratkaisuja. Päivittäiset valvonta- ja häiriöprosessit yhdistettynä tehokkaisiin teknologiaratkaisuihin vahvistavat ns. ”kybersietoisuutta” ja ratkaisut toimivat sellaisenaan varautumisessa yhteiskunnan kannalta poikkeustilanteisiin.

Julkisten palvelujen tulee olla luotettavia, mutta lisäksi niiden tulee olla käyttäjäystävällisiä ja tukea kyberturvallista käyttöä. Julkisten palveluiden vaatimuksenmukaisuuden tulisi pohjautua selkeästi yhtenevään kriteeristöön, joka pohjautuu yleiseen ja ylläpidettyyn standardiin tai säädökseen. Toimialakohtaisesti viranomaisen tulee täydentää/tarkentaa vaatimuksia toimialaan sopiviksi ja kerätä parhaita käytäntöjä.

Kyberrikollisuuden ehkäiseminen nojaa välttämättä yhteiskunnan kaikkien toimijoiden aktiiviseen toimintaan. Tämä tulisi kuvata selkeämmin tavoitteessa (ennaltaehkäistään kyberrikollisuutta).

Tilanneymmärrystä korostetaan useasti ja osin tarpeettomasti sekä varautumisen, että myös Nykytila-, Yhteystoiminta- sekä Reagointi- ja vastatoimet -luvuissa. Tilanneymmärrys on tarpeellinen monella tasolla ja -toiminteessa, mutta samalla sitä tulisi pitää itsestäänselvyytenä, mikäli aikomuksena on rationaalinen toiminnan ohjaaminen. Tilanneymmärrystä voidaan hyödyntää tietoperusteisesti oikeiden ja oikeasuhtaisten toimenpiteiden valinnalle, mutta tilanneymmärrys sinänsä ei luo tavoiteltua muutosta. Nyt esitetty ilmaisutapa ja toistojen määrä voi luoda virheellisen käsityksen, että on tarpeen käyttää mittavia resursseja yksinomaan tilanneymmärryksen kehittämiseksi. Teknisessä mielessä tilanneymmärryksen tuottamiseksi on tarpeen ylläpitää yhteen toimivaa ja käyttökustannuksiltaan kohtuullista ratkaisua (eri toimittajien tuotteista). Päällekkäisiä ratkaisuja ei ole perusteltua ylläpitää eri viranomaisissa, vaan perustaa toiminta kokonaiskuvan osa-alueiden jakamiseen lain sallimissa rajoissa.

Automaattinen tekninen seuranta ja valvonta ovat avainasemassa kyberturvallisuuden tilannekuvan ja turvallisuuden mahdollistamiseksi. Tätä tulisi painottaa voimakkaammin.

Ehdotamme, että virke ”Suomi varautuu kyberuhkiin ennakoivasti.” kirjoitetaan muotoon: ”Suomessa hallitaan kyberturvallisuusriskejä vakavien seurausten välttämiseksi.” (s. 26).

Kokonaisuudessaan strategialuonnos vaikuttaisi kytkevän kyberturvallisuuteen liittyvän varautumisen koordinaation valtion kyberturvallisuusjohtajan toimintoon. Samalla kuitenkin luonnoksessa Yhteiskunnan turvallisuusstrategiasta (YTS) todetaan varautumisesta, että *”sitä johtaa, valvoo ja yhteensovittaa kukin ministeriö toimialallaan.”* YTS:n kirjaus vaikuttaa vastaavan nykyistä oikeustilaa sekä hallinnon toimintaa, joten on perusteltua, että kyberturvallisuuden strategiassa ilmaistaan, onko oikeustilaa tarkoitus muuttaa ja miltä osin, esim. Valtion kyberturvallisuusjohtajan tehtävän vahvistaminen X ja Y osalta.

Kannatamme vahvasti (s.29) kirjausta *”Viranomaisen mahdollisuus tarjota kyberturvallisuuspalvelu asiakkaille maksullisena palveluna on selvitettävä aina uutta palvelua käyttöönotettaessa.”* Toteamme kuitenkin, että myös maksullisen viranomaispalvelun käyttäminen voi pienillä markkinoilla johtaa yksityisen sektorin pienenemiseen eivätkä vahvista tervettä kyberturvallisuusteollisuuden markkinaa. Viranomaisen maksulliset palvelut voivat olla hinnoiteltu yksinomaan tuotantokustannusten mukaan, tai jopa alle, jolloin kaupallisin perustein toimivat organisaatiot eivät pysty kilpailemaan. Kirjattuna periaatteena tulisikin olla, että viranomaisen ei tule luoda toimintoja tai palveluita, joiden osalta on olemassa toimiva markkina tai joka voidaan luoda sääntelyn sekä muiden kannusteiden avulla.

Pienillä markkinoilla homogeeniset, keskitetysti ostetut ratkaisut johtavat yksityisen sektorin pienenemiseen eivätkä ruoki tervettä yksityissektorin kyberturvallisuusteollisuutta. Usein kilpailutuksissa hinta on myös 100% valintakriteeri.

Yhteenveto:

- Varautumisen toimijuus tulisi kuvata kattavammin ja perustellummin.
- Soveltuvien kyberturvallisuuden riskienhallintakeinojen käyttöönottaminen ja kehittäminen tulisi nostaa keskeisimmäksi tavoitteeksi.
- Tilanneymmärryksen toistamista ja siten myös sen merkityksen ylikorostumista tulisi välttää.
- Viranomaisten ei tule luoda toimintoja tai palveluita, joiden osalta on olemassa toimiva markkina tai joka voidaan luoda sääntelyn sekä muiden kannusteiden avulla.

III Yhteistoiminta

Viranomaisten intressien hahmottamisessa olisi perusteltua ottaa jo lähtökohdaksi se, millaiset politiikkatoimet olisivat Suomen pitkäaikaisen kokonaisedun mukaisia. Sen lisäksi, mitä strategialuonnoksessa on jo ansiokkaasti esitetty, toiminnan periaatteeksi tulisi kirjata myös, miten Suomi kehittyy, kilpailee ja pärjää suhteessa muihin valtioihin (välttäen hallinnonalojen omia, osaoptimoituja kehittämiskeinoja). On välttämätöntä, että Suomen asema avoimena sekä yritysten oikeuksia ja intressejä kunnioittavana markkinataloutena otetaan aiempaa selvemmin huomioon myös digitaalisen turvallisuuden toimissa.

Strategialuonnoksessa ehdotuksen mukaisesti *”Julkinen ja yksityinen sektori kehittävät tiiviimpää ja luottamusta vahvistavaa yhteistoimintamallia”*, tulisi strategiassa ottaa kantaa myös siihen, millaisilla rakenteilla tavoitetta kohdin edetään. Kyseistä tavoitetta koskevassa luvussa kehittäminen vaikuttaa kohdistuvan pääosin, ellei lähes kokonaan viranomaisten toiminnan ja

yhteistyömuotojen kehittämiselle. Lisäksi yhteistyö vaikuttaa kohdistuvan lähinnä kyberuhkia koskevaan tiedonvaihtoon eli häiriötilanteiden hallintaan, mikä edustaa vain yhtä, kapeahkoa yhteistoiminnan osa-aluetta yhteensä yhdeksästä jo aiemmin tunnistetusta alueesta (ohjaus, tutkimus, tilannekuva, regulaatio, osaaminen, jatkuvuus/varautuminen, hankinnat/hankkeet/palvelut, harjoittelu).

Luottamusta vahvistavaa yhteistoimintamallia ei ole mahdollista saavuttaa yksistään kuvatuilla toimintalinjoilla tai ehdotetulla rakenteella (liitteessä kuvattuna). Tästä syystä strategiassa olisikin perusteltua ottaa kantaa, miten kyberturvallisuuden kehittämistä tultaisiin ohjaamaan ja keskustelua käymään. Luvusta puuttuu myös kokonaan pohdinta siitä, mitkä ovat yksityisen sektorin intressit ja mahdollisuudet tukea ja osallistua viranomaisten toimintaa kuvaaviin tavoitteisiin. Yhteistoiminnan luonnostelussa tulisi lähteä liikkeelle siitä, miten strategia mahdollistaa hallitusohjelmassakin vahvistetun tavoitteen, jossa poliittisen- ja hallintovallan tehtävä on tarjota puitteet vapaudelle ja (taloudellisille) mahdollisuuksille.

Katsomme, että strategian tässä osiossa yhteistoiminnan näkökulmasta on tarpeen ottaa kantaa mm. Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvityksen (2022) tavoitetilaa sekä keskeisimpiä kehitysehdotuksia koskeviin seikkoihin (sovitettuna nykyisiin ministeriryhmiin ja -työnjakoon).

Strategialuonnoksen liitteessä on kuvattu yhteiskunnan eri toimijat kansallisen kyberturvallisuuden varmistamisessa. Kuvaus on sinänsä kattava, muttei vastaa oikeudellista todellisuutta tai yhteiskunnan toiminnan kannalta mielekästä hahmottelua vastuista. Suomen n. 450 000 yrityksestä 20 suurimman yhteenlaskettu liikevaihto ylittää yksinään 160 mrd€ (lähes kaksi kertaa valtion 2024 budjetti) ja esim. teknologia-alan 6000 yritystä muodostavat noin kolmanneksen Suomen bruttokansantuotteesta. Tässä valossa on syytä painottaa, että yhteistyörakenteissa, joissa ei ole elinkeinoelämän kattavaa edustusta on ilmeinen vaara, että vaikuttavuus (strategian tavoittelemalla tavalla) jää heikoksi kansallisen kyberturvallisuuden kehittämisen, suunnittelun, varautumisen ja kriittisen tieto- ja viestintäteknisen infrastruktuurin varautumisen koordinaation ja yhteensovittamisen osalta. Kyse ei siis ole yksinomaan siitä, että elinkeinoelämän edustajat osallistuisivat erilaisiin yhteistyöryhmiin vain julkisen ja yksityisen sektorin välisen luottamuksen rakentamisen vuoksi.

Myös ns. valvovien viranomaisten kokonaisuus on vaarassa jäädä karkeaksi yleiskuvaukseksi ja heikosti perustelluksi ”toiminnalliseksi” osaksi, sillä Suomessa hallintoviranomaiset toimivat itsenäisesti julkista hallintotehtävää hoitaessaan ja hallintopäätöksiä tehdessään. Ministeriöllä on toimivalta antaa alaiselleen hallinnolle yleisiä tulkinnallisia, ei-sitovia ohjeita lainsäädännön sisällöstä ja soveltamisesta sekä menettelytapavaatimuksista.

Yhteenveto:

- Politiikkatoimissa tulisi ottaa huomioon Suomen pitkäaikainen hallinnonalat ylittävä kokonaisetu ja siten välttää osaoptimoituja kehittämiskeinoja.
- Korostetaan Suomen asemaa avoimena markkinataloutena myös digitaalisen turvallisuuden toimissa.
- ”Yhteistoimintamallia” tulisi laajentaa kattamaan kaikki tunnistetut yhteistoiminnan osa-alueet ja sisällyttää yksityinen sektori osaksi toimintaa.

IV Reagointi ja vastatoimet

Yhteiskunnan perustoiminnot sekä taloudellisen toimeentulon jatkuvuus nojaavat yksityisen elinkeinoelämän toimintaan. Näin ollen kansallisen turvallisuuden keskeinen toimijajoukko on

elinkeinoelämä eritoten huoltovarmuuteen, vientiin ja teknologiaan liittyvät yritykset. Tämän vuoksi myös yhteiskunnan kyberkestävyyden vahvistamisen kannalta tärkeimmät askeleet otetaan yrityksissä, joiden hallussa on suurin osa tietojärjestelmistä sekä tiedosta. On hyvä huomioida, että pelkästään työnantajayrityksiä on Suomessa noin kaksisataa kertaa ja huoltovarmuuskriittisiä yli kymmenen kertaa enemmän kuin julkishallinnon organisaatioita.

Strategialuonnoksessa todetaan, että kyberdiplomatian, -puolustuksen ja -turvallisuuden toimilla vastataan kyberuhkiin. Lähtökohta asettaa avoimeksi sen, mitä tosiallisesti aiotaan tavoitella kyberdiplomatian ja -puolustuksen osa-alueilla. Strategian tavoitelaajuuden näkökulmasta jää kysymys, mikä on (kansallisen) kyberturvallisuuden ja kansallisen kyberpuolustuksen ero, kun kummatkin kattavat myös ns. ”siviilialojen” toimet myös (valtioiden) kyberuhkia ja -häiriöitä vastaan.

Reagointi- ja vastatoimet -luvussa ylikorostuu sotilaallisen maanpuolustuksen ja julkisen hallinnon toimijoiden rooli kyberuhkien torjunnassa. Yleisen kyberturvallisuuden ja kansallisen kyberpuolustuksen eroavaisuudet ovat huomattavasti pienempiä, kuin mitä strategialuonnos antaa ymmärtää. Mikäli digitaalinen turvallisuus käsitetään vain kyberpuolustuksen näkökulmasta, on riskinä, ettei resursseja kohdenneta optimaalisella tavalla. Tietoturvaloukkausten (ml. tietomurrot, tietoliikenteen häirintä ja datavahingonteot) keinot ja työkalut ovat pitkälti samoja oli sitten kyseessä valtiollinen toiminta tai muu rikollinen toiminta. Tekijästä riippumatta hyökkäykset hyödyntävät samoja ohjelmistojen ja konfiguraatioiden haavoittuvuuksia, jolloin torjunnan etulinjassa ovat kaikkien organisaatioiden tietoturvallisuusvastaavat. Myös vieraiden valtioiden toimia torjutaan laajasti nimenomaan tieto- eli kyberturvallisuuden (ml. pakolliset teknishallinnolliset tietoturvallisuusvaatimukset), lainvalvonnan ja rikosprosessin sekä osin diplomaattisin toimin. Ns. kyberpuolustus onkin pääosin kyberturvallisuuden riskienhallintakeinojen hallintaa ja rikosten torjuntaa.

Epäselväksi jää myös, miksi ”Valtiollisiin kyberoperaatioihin reagoidaan ja vastataan eri tavoin kuin tavanomaisiin kyberuhkiin.” Mikäli erilainen lähestymistapa olisi tarpeen, strategiassa tulisi ottaa kantaa siihen, millä tavalla ”valtiolliset kyberoperaatiot” eroavat laittomista tietoturvaloukkauksista muuten kuin, että tekijät saattavat olla valtion virkahenkilöitä tai niiden ohjauksessa. Tarkan ja perusteltavissa olevan attribuution (vastuun osoittamisen) yksi olennaisimmista elementeistä on tietoturvaloukkauksen kohteessa suoritettava IT-forensiikka, ja sitä tukevat ruohonjuuritason IT-prosessit kuten lokien käsittely, turvatapahtumien analysointi ja hyökkäyksen tunnuspiirteiden tunnistamisen lokimassoista (Indicators of Compromise, IoC).

Lisäksi on perusteltua suhtautua suurella varauksella väitteeseen, että ”*Valtiolliseen vihamieliseen kybertoimintaan vastaaminen rikosvastuuseen saattamisen menetelmin ei välttämättä ole tehokkain tapa.*” Esimerkiksi Yhdysvaltojen kyberturvallisuusstrategiassa nojaudutaan juuri päinvastaiseen ja menettelytavan vaikuttavuudesta on saatavilla tietoa. Vastaavasti ”aktiivisen kyberpuolustuksen” hyödyistä ei ole kansallisesti esitetty vastaavaa näyttöä. Strategian tasolla olevien toimintalinjojen valinnan tulee perustua parhaaseen ymmärrykseen, kattavaan arviointiin, kansainvälisen oikeuden mukaiseen harkintaan ja yleiseen hyväksyttävyyteen. Verrannollisesti Suomessa esimerkiksi sisäisen turvallisuuden strategiatyössä ei ole esitetty, että (sota- eli puolustustila pois lukien) kolmannen valtion kansalaisen Suomessa toteuttama tuhotyörikoksen tulisi johtaa siihen, että suomalainen viranomainen toteuttaisi vastaavan rikoksen tekijän lähtömaassa, vaikka olisi tiedossakin, että kyseinen taho olisi saanut ohjauksen, ohjeen tai motivaation tältä lähtövaltiolta. Erillinen asia on toiminta, jossa lainvalvontaviranomainen suorittaa laittomassa käytössä olevien palveluiden tai laitteistojen alasajon ja/tai haltuunoton selvien ja kiistattomien kansainvälisten oikeussääntöjen puitteissa.

Tietoturvaloukkausten tunnistaminen on alkuvaiheessa erittäin vaikeaa. Vastuuta ei voi eikä tule määrittää hyökkäyksen toimijan tai tämän oletetun motivaation kannalta, vaan estävien ja korjaavien toimenpiteiden toteuttamisen näkökulmasta.

Suomessa on tarve kyberpuolustukseen liittyville toimille ja on kannatettavaa, että tätä koskeva kyberpuolustusdoktriini laaditaan erikseen ja että siinä käsitellään rauhan, kriisin ja konfliktin oloihin liittyvät seikat. Tässä kontekstissa, kuten lausunnossa on aiemmin todettu, motivaatioihin liittyvät termit kuten ”vihamielisyys” jättävät lähinnä lukijan tunteiden varaan sen, miten vihamielisyys ilmenee. Erityisen tärkeää on se, että Suomessa hyödynnetään kattavasti kansallista keinovalikoimaa niin, että toimien voidaan osoittaa vaikuttavan myönteisesti kyberturvallisuusriskien vähenemiseen.

Luvusta puuttuu kokonaan EU:n kybersolidaarisuussäädöksen aiheuttamat muutokset ja tavoitteiden vaikutus kansalliselle tasolle (vrt. NIS2-direktiiviä koskeva osuus).

Yhteenveto:

- Kyberpuolustuksen ja kyberdiplomatian tavoitteita tulisi selventää.
- Valtiollisten kyberoperaatioiden ja laittomien tietoturvaloukkauksien ero tulisi kuvata sellaisella selkeydellä, että strategian linjaukset voidaan perustella oikeusvaltion toimintakehyksessä.
- Selkeytetään strategian rakenteessa, miten kyberrikollisuuden ennaltaehkäisy (pilari II s. 26) eroaa tässä luvussa esitetystä kyberrikollisuuden torjunnasta.
- EU:n kybersolidaarisuussäädöksen vaikutukset kansalliselle tasolle tulisi huomioida NIS2-direktiiviä vastaavalla tavalla.

Resursointi, toimeenpano ja seuranta

Strategian resursointi, toimeenpano ja seuranta ovat onnistumisen kannalta keskeisiä. Strategian toimeenpanoon kytketyt resurssit määrittävät sen, kuinka strategiassa esitettyihin tavoitteisiin päästään. Strategiassa, tai sen toimeenpano-osassa olisi perusteltua olla tavoitellut toimet priorisoituna ja osoitettuna toimijat, vastuut ja resurssit.

Kansainvälistä rahoitusta koskevassa osioissa tulisi käyttää termiä ”TKI-rahoitus” vakiintuneen käytännön mukaisesti ja että EU:n toimet ja instrumentit mainitaan ensin ja selvästi merkittävämpänä kokonaisuutena NATOn rahoitukseen nähden. Digitaalisen ja kyberturvallisuuden kehittämiseen liittyvä rahoitus niin instrumenttien kuin rahoituksen määrän osalta on EU:n osalta moninkertaista.

Hallitusohjelmassa ja Suomen digitaalisessa kompassissa kirjattu yhteiskehitysbudjetti tulee hyödyntää tehokkaasti myös kyberturvallisuuden parantamiseen. Yhteiskehitysbudjetin avulla voidaan keskittää resursseja ja varmistaa, että hankkeet ovat linjassa hallitusohjelman prioriteettien kanssa sekä yhteen toimivia koko valtionhallinnon digitaalisen infrastruktuurin ja digitalisaatiokehityksen kanssa. Samalla tuettaisiin yllä ehdotetun kansallisen kyberturvallisuuden TKI-ohjelman tavoitteita.

Yhteenveto:

- Strategian toimeenpanotoimet ja niille osoitetut resurssit tulisi priorisoida tärkeys- tai painopistejärjestykseen.
- Termiä "TKI-rahoitus" tulisi käyttää kansainvälisestä rahoitusta koskevassa kuvauksessa.
- EU-rahoitusinstrumentteja tulisi korostaa selvästi suhteessa NATO:n vastaaviin.

Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

- Hallitusohjelmaan kirjattu ministeriöiden välinen yhteiskehitysbudjetti tulee hyödyntää myös kyberturvallisuuden parantamiseen.

Lisätiedot

Peter Sund, Kyberala ry, +358 50 565 0621, peter.sund@teknologiateollisuus.fi

Risto Rajala, +358 40 5156187, risto.rajala@teknologiateollisuus.fi