Euroopan unionin neuvosto

Bryssel, 13. syyskuuta 2018
(OR. en)

12104/18
ADD 5

Toimielinten välinen asia:
2018/0328(COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

SAATE

Lähettäjä:	Euroopan komission pääsihteerin puolesta Jordi AYET PUIGARNAU, johtaja
Saapunut:	12. syyskuuta 2018
Vastaanottaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	SWD(2018) 404 final
Asia:	KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA TIIVISTELMÄ VAIKUTUSTEN ARVIOINNISTA Oheisasiakirja EHDOTUS EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta

Valtuuskunnille toimitetaan oheisena asiakirja SWD(2018) 404 final.

Liite: SWD(2018) 404 final

EUROOPAN
KOMISSIO

Bryssel 12.9.2018
SWD(2018) 404 final

KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA

TIIVISTELMÄ VAIKUTUSTEN ARVIOINNISTA

Oheisasiakirja

EHDOTUS EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Vaikutustenarvioinnin tiivistelmä

Vaikutustenarviointi: Ehdotus osaamiskeskusten verkoston ja Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen perustamisesta

A. Toimenpiteen tarve

Miksi? Mihin ongelmaan puututaan?

EU:lta puuttuu edelleen riittävät teknologiset ja teolliset valmiudet, jotta se voisi itsenäisesti turvata taloutensa ja kriittiset infrastruktuurinsa ja saavuttaa maailmanlaajuisen johtoaseman kyberturvallisuuden alalla. Nyt ehdotettavalla aloitteella pyritään edistämään puuttumista seuraaviin tähän tilanteeseen vaikuttaviin ongelmiin ja niiden taustatekijöihin:

Ongelma 1: Riittämätön strateginen ja kestävä koordinointi ja yhteistyö teollisuuden, kyberturvallisuuden tutkimusyhteisöjen ja julkishallintojen välillä talouden, yhteiskunnan ja demokratian suojaamiseksi viimeisintä kehitystä edustavilla kyberturvallisuusratkaisuilla.

Ongelma 2: Riittämättömät investoinnit ja rajalliset mahdollisuudet saada käyttöön kyberturvallisuusalan taitotietoa, osaamista ja välineitä Euroopassa.

Ongelma 3: Vain harvat eurooppalaiset kyberturvallisuusalan tutkimus- ja innovointitulokset muunnetaan markkinoitaviksi ratkaisuiksi ja otetaan laajasti käyttöön taloudessa.

Näihin ongelmiin vaikuttaa joukko taustatekijöitä, joita ovat muun muassa puutteellinen luottamus kyberturvallisuusmarkkinoiden eri toimijoiden välillä, olemassa olevien yhteistyömekanismien ja rahoituksen kokoamismekanismien luontaiset rajoitukset, kehyksen puuttuminen kalliiden kyberturvallisuusinfrastruktuurien ja kyberturvallisuustuotteiden/-ratkaisujen yhteisiltä hankinnoilta sekä markkinoiden push-pull-mekanismien tarjoamien mahdollisuuksien hyödyntämättä jättäminen.

Mitä toimenpiteellä on tarkoitus saada aikaan?

Aloitteella pyritään varmistamaan, että EU pitää yllä ja kehittää olennaisia (teknologisia ja teollisia) valmiuksia, jotta se voi itsenäisesti turvata digitaalisen taloutensa, yhteiskuntansa ja demokratiansa ja jotta jäsenvaltiot voivat hyötyä kehittyneimmistä kyberturvallisuusratkaisuista ja kyberpuolustusvalmiuksista. Aloitteella pyritään myös parantamaan EU:n kyberturvallisuusalan yritysten maailmanlaajuista kilpailukykyä ja varmistamaan, että Euroopan eri teollisuudenaloilla on mahdollisuus saada käyttöönsä valmiuksia ja resursseja, joiden avulla ne voivat tehdä kyberturvallisuudesta itselleen kilpailuedun. Tämä on määrä saavuttaa kehittämällä toimivat mekanismit kaikkien asianomaisten toimijoiden (viranomaiset, teollisuus ja tutkimusyhteisö sekä siviili- että puolustusalalla) pitkän aikavälin strategiselle yhteistyölle, kokoamalla yhteen tietämystä ja resursseja viimeisintä kehitystä edustavien valmiuksien ja infrastruktuurien tarjoamiseksi, edistämällä eurooppalaisten kyberturvallisuustuotteiden ja -ratkaisujen laajaa käyttöönottoa taloudessa ja julkisella sektorilla, tukemalla kyberturvallisuusalan startup-yrityksiä ja pk-yrityksiä sekä auttamalla poistamaan kyberturvallisuuteen liittyvän osaamisvajeen.

Mitä lisäarvoa saadaan toimenpiteen toteuttamisesta EU:n tasolla?

Aloite lisäisi nykyisten kansallisen tason toimien arvoa auttamalla luomaan Euroopan laajuisen yhteenliitetyn kyberturvallisuusalan teollisuus- ja tutkimusekosysteemin. Sen pitäisi edistää parempaa yhteistyötä asianomaisten sidosryhmien välillä (myös kyberturvallisuuden siviili- ja puolustussektoreiden välillä), jotta ympäri Eurooppa hajautuneita olemassa olevia kyberturvallisuusvalmiuksia ja osaamista voitaisiin hyödyntää mahdollisimman tehokkaasti. Sen pitäisi auttaa EU:ta ja jäsenvaltioita omaksumaan kyberturvallisuusalan teollisuuspolitiikkaan proaktiivinen, pidemmälle aikavälille suuntautuva ja strateginen näkökulma, joka ulottuu pelkkää tutkimusta ja kehittämistä laajemmalle. Tämän lähestymistavan pitäisi helpottaa läpimurtoratkaisujen löytämistä yksityisen ja julkisen sektorin kohtaamiin kyberturvallisuushaasteisiin sekä tukea näiden ratkaisujen tehokasta käyttöönottoa. Se antaa myös asianomaisille tutkimus- ja teollisuusyhteisölle sekä viranomaisille mahdollisuuden saada käyttöönsä keskeisiä valmiuksia, kuten testaus- ja kokeilujärjestelyjä, jotka ovat usein yksittäisten jäsenvaltioiden ulottumattomissa niiden riittämättömien taloudellisten ja henkilöresurssien vuoksi. Se edistää myös osaamisvajeen poistamista ja aivovuodon ehkäisemistä varmistamalla parhaille kyvyille mahdollisuuden osallistua suuren mittakaavan eurooppalaisiin hankkeisiin ja siten tarjoamalla mielenkiintoisia ammatillisia haasteita. Kaikkia edellä mainittuja näkökohtia pidetään myös välttämättöminä, jotta unioni tunnustettaisiin maailmanlaajuiseksi johtajaksi

kyberturvallisuuden alalla.

B. Ratkaisut

Mitä lainsäädännöllisiä ja muita toimenpidevaihtoehtoja on harkittu? Onko jokin vaihtoehto arvioitu parhaaksi? Miksi?

Vaikutustenarvioinnissa tarkasteltiin useita toimintavaihtoehtoja, sekä lainsäädännöllisiä että muita. Perinpohjaiseen arviointiin otettiin seuraavat vaihtoehdot:

1. **Perusskenaariossa** – yhteistyöhön perustuvassa vaihtoehdossa – oletetaan, että nykyistä lähestymistapaa kyberturvallisuuteen liittyvien teollisten ja teknologisten valmiuksien kehittämiseen jatketaan tukemalla tutkimusta ja innovointia ja siihen liittyviä yhteistyömekanismeja Euroopan horisontti -ohjelmassa.
2. **Vaihtoehto 1:** Perustetaan kyberturvallisuuden osaamisverkosto ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus, jolla on valtuudet viedä eteenpäin toimenpiteitä teollisuusteknologioiden sekä tutkimuksen ja innovoinnin tukemiseksi.
3. **Vaihtoehto 2:** Perustetaan kyberturvallisuuden osaamisverkosto ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus, jotka keskittyvät ainoastaan tutkimus- ja innovointitoimiin.

Varhaisessa vaiheessa hylättiin seuraavat vaihtoehdot: 1) ei mitään toimenpiteitä, 2) ainoastaan olemassa olevien osaamiskeskusten verkosto ja 3) olemassa olevien virastojen käyttäminen (ENISA, REA tai INEA).

Kun otetaan huomioon komission jo ilmaisema yleinen sitoutuminen tähän aloitteeseen sekä jäsenvaltioiden merkittävä osuus siinä, kahden perusteellisesti analysoidun toimintavaihtoehdon suurin ero liittyy niiden soveltamisalaan, mikä näkyy niiden oikeusperustassa: ainoastaan SEUT-sopimuksen 187 artiklaan perustuva elin (vaihtoehto 2) rajoittaisi aloitteen tutkimuksen ja innovoinnin alaan, ja se edellyttäisi tyypillisesti yksityisen sektorin toimijoiden rahoitusta. Kahtalaiseen oikeusperustaan – SEUT-sopimuksen 187 artikla ja 173 artikla – perustuva elin (vaihtoehto 1) puolestaan merkitsisi laajempaa toimeksiantoa, joka kattaisi muun muassa käyttöönoton ja teollisuuden tukemisen sekä vahvempien synergioiden luomisen kyberpuolustuksen kanssa. Jäsenvaltiot olisivat siinä merkittävämmässä asemassa sekä hallinnon osalta että kyberturvallisuusteknologian potentiaalisina hankkijoina.

Analyysissa todettiin, että aloitteen tavoitteet saavutetaan parhaiten vaihtoehdolla 1. Sillä saavutetaan myös suurin taloudellinen, yhteiskunnallinen ja ympäristövaikutus ja turvataan unionin edut. Tärkeimpiä tätä vaihtoehtoa tukevia näkökohtia olivat joustavuus, joka mahdollistaa erilaiset yhteistyömallit osaamisyhteisön ja osaamiskeskusten verkoston kanssa, jotta olemassa olevaa tietämystä ja resursseja voidaan hyödyntää parhaalla mahdollisella tavalla; kyky strukturoida kaikilta asiaan liittyviltä aloilta, myös puolustuksen alalta, tulevien julkisten ja yksityisten sidosryhmien yhteistyö; sekä kyky luoda todellinen kyberturvallisuusalan teollisuuspolitiikka tukemalla toimia, jotka eivät liity ainoastaan tutkimukseen ja kehittämiseen, vaan myös markkinoille saattamiseen. Vaihtoehto 1 lisää myös koherenssia, kun se toimii täytäntöönpanomekanismina Digitaalinen Eurooppa -ohjelmasta ja Euroopan horisontti -ohjelmasta annattavalle kyberturvallisuuteen liittyvälle rahoitukselle, ja se parantaa kyberturvallisuuden siviili- ja puolustusulottuvuuksien välisiä synergioita suhteessa Euroopan puolustusrahastoon.

Mitkä toimijat kannattavat mitäkin vaihtoehtoa?

Kuulemis- ja tiedonkeruuprosessien tulosten perusteella sekä teollisuus- että tutkimusyhteisöissä on selkeä tarve mekanismille, joka mahdollistaa tutkimus- ja kehitystoimia laajemmalle ulottuvan EU:n johdonmukaisen teollisuuspolitiikan kyberturvallisuusalalla. Ainoastaan näin voidaan mahdollistaa se, että Eurooppa saavuttaa maailmanlaajuisen johtoaseman kyberturvallisuuden alalla. Samaan aikaan sidosryhmät korostivat, että onnistumisen kannalta keskeistä on osaamiskeskuksen tarkasti määritelty rooli verkoston ja asianomaisten yhteisöjen toimien tukijana ja helpottajana sekä kattava, yhteistyöhön perustuva lähestymistapa lokeroitumisen välttämiseksi. Rakenteen olisi myös oltava joustava, jotta sitä voidaan mukauttaa helposti, koska kyberturvallisuus on nopeasti kehittyvä ala. Jäsenvaltiot korostivat koko prosessin ajan, että kaikilla jäsenvaltioilla ja niiden nykyisillä osaamiskeskuksilla tulisi olla mahdollisuus osallistua osaamisverkostoon ja että erityistä huomiota olisi kiinnitettävä toimien täydentävyyteen. Osaamiskeskuksen osalta jäsenvaltiot korostivat sen koordinoivan roolin merkitystä verkoston tukemisessa. Komission aloitteessa on siten löydettävä oikea tasapaino hallinto- ja

täytäntöönpanorakenteissa ja varmistettava näin tehokas koordinointi unionin tasolla ottaen samalla huomioon kansallisen tason kehitys.

C. Parhaaksi arvioidun vaihtoehdon vaikutukset

Mitkä ovat parhaaksi arvioidun vaihtoehdon hyödyt (jos parhaaksi arvioitua vaihtoehtoa ei ole, päävaihtoehtojen hyödyt)?

Parhaaksi arvioitu vaihtoehto antaa kaikkien jäsenvaltioiden viranomaisille ja yrityksille paremmat mahdollisuudet ehkäistä kyberuhkia ja reagoida niihin, kun ne voivat tarjota ja ottaa käyttöön turvallisempia tuotteita ja ratkaisuja. Tämä on erityisen tärkeää keskeisten palvelujen saatavuuden turvaamiseksi (esim. liikenne, terveydenhuolto, pankki- ja rahoituspalvelut). Sillä olisi myös myönteinen vaikutus EU:n kilpailukykyyn ja pk-yrityksiin, sillä siinä luotaisiin mekanismi, joka mahdollistaa jäsenvaltioiden ja unionin kyberturvallisuusalan teollisten valmiuksien kehittämisen ja Euroopan tieteellisen huippuosaamisen tehokkaan muuntamisen markkinoille saatettaviksi ratkaisuiksi, jotka voidaan ottaa käyttöön kaikkialla taloudessa. Vaihtoehto mahdollistaa resurssien yhdistämisen, jotta tarvittaviin valmiuksiin voidaan investoida jäsenvaltioiden tasolla ja kehittää yhteisiä eurooppalaisia voimavaroja ja saavuttaa mittakaavaetuja. Tämän pitäisi lisätä pk-yritysten, teollisuuden ja tutkijoiden mahdollisuuksia saada käyttöönsä tällaisia valmiuksia, mikä edistää innovointia ja lyhentää kehitysprosesseja. Tämä pienentää myös eräiden kysyntäpuolen yritysten kustannuksia ja auttaa niitä tekemään kyberturvallisuudesta itselleen kilpailuedun. Vaihtoehto mahdollistaa kaksikäyttöteknologioiden markkinamahdollisuuksien hyödyntämisen, kun puolustus- ja siviilialan yhteisöt voivat tehdä yhteistyötä yhteisissä haasteissa. Sen pitäisi myös antaa lisäarvoa kansallisille toimille, joilla pyritään supistamaan kyberturvallisuuteen liittyvää osaamisvajetta. EU:n tasolla vaihtoehto mahdollistaa eri rahoitusmekanismien yhdenmukaisuuden ja niiden välisten synergioiden parantamisen.

Välillinen myönteinen vaikutus ympäristöön voitaisiin saavuttaa kehittämällä erityisiä kyberturvallisuusratkaisuja aloille, joilla on potentiaalisesti mittava ympäristövaikutus (esim. ydinvoimalat), ja auttamalla niitä välttämään niiden infrastruktuuriin kohdistuvien kyberhyökkäysten mahdollisesti katastrofaaliset seuraukset.

Mitkä ovat parhaaksi arvioidun vaihtoehdon kustannukset (jos parhaaksi arvioitua vaihtoehtoa ei ole, päävaihtoehtojen kustannukset)?

Parhaaksi arvioidun vaihtoehdon kustannukset liittyvät pääasiassa osaamiskeskuksen ja kansallisten koordinointikeskusten toimintaan. Eri rahoitusohjelmien (Digitaalinen Eurooppa -ohjelma ja Euroopan horisontti -ohjelma) toteuttamiseen liittyvistä kustannuksista on tehty erilliset vaikutustenarvioinnit.

Mitkä ovat vaikutukset yrityksiin, mukaan lukien pk- ja mikroyritykset?

Suurimmat vaikutukset kohdistuvat sekä kysyntä- että tarjontapuolella toimiviin kyberturvallisuusalan eurooppalaisiin yrityksiin, myös pk- ja mikroyrityksiin. Vaikka osaamiskeskuksen ja verkoston perustaminen ei aiheuta yrityksille lakisääteisiä vaatimuksia, se avaa mahdollisuuksia kustannusten vähentämiseen uusien tuotteiden suunnittelussa ja auttaa niitä luomaan yhteyksiä sijoittajiin ja hankkimaan markkinakelpoisten ratkaisujen käyttöönotossa tarvittavaa rahoitusta. Pk- ja mikroyritysten tapauksessa mahdollisuus käyttää julkisesti rahoitettuja testaus- ja kokeilujärjestelyjä on vieläkin tärkeämpää, koska näillä yrityksillä ei ole resursseja hankkia käyttöönsä tarvittavaa infrastruktuuria tai saada siihen pääsyä omien markkinoidensa (ja usein EU:n) ulkopuolella. Aloitteen toivotaan myös avaavan uusia markkinoita kyberturvallisuuden alalla toimiville eurooppalaisille pk- ja mikroyrityksille. Valittu mekanismi varmistaa myös koordinoinnin tutkimusyhteisön ja teollisuuden välillä ja ohjaa siten tutkimustoimia kohti teollisuuden konkreettisia tarpeita. Huipputason kyberturvallisuusosaamisen ja -työkalujen tarjoaminen auttaa välillisesti talouden toimijoita verkko- ja tietoturvadirektiivin noudattamisessa.

Kohdistuuko jäsenvaltioiden budjettiin ja julkishallintoon merkittäviä vaikutuksia?

Aloitteen avulla jäsenvaltiot voivat koordinoida tarvittavaan kyberturvallisuusinfrastruktuuriin kansallisella ja unionin tasolla tehtäviä investointeja. Mekanismi mahdollistaa resurssien kokoamisen sellaisia työkaluja ja infrastruktuureja varten, jotka muutoin olisivat kalliimpia tai yksittäisten jäsenvaltioiden ulottumattomissa. Tällainen lähestymistapa mahdollistaisi mittakaavaedut ja järkeistämisen. Jäsenvaltioiden rahoitusosuuden osaamiskeskukseen ja siihen liittyviin toimiin olisi oltava samansuuruinen kuin unionin osuus.

Onko toimenpiteellä muita merkittäviä vaikutuksia?

Aloitteella on selkeä myönteinen vaikutus, sillä sen pitäisi lisätä merkittävästi jäsenvaltioiden kykyä turvata

itsenäisesti omat taloutensa ja suojata kriittiset sektorit. Se myös parantaa Euroopan kyberturvallisuusalan yritysten sekä muiden alojen yritysten kilpailukykyä, kun ne voivat asianmukaisesti suojata käyttämänsä omaisuuden ja suunnitella turvallisia innovatiivisia tuotteita pienentäen samalla turvallisuuteen liittyviä t&k-kustannuksia. Tämän pitäisi viime kädessä mahdollistaa se, että EU ottaa johtoaseman seuraavan sukupolven digitaali- ja kyberturvallisuusteknologioiden alalla.

D. Seuranta

Milloin asiaa tarkastellaan uudelleen?

Säädökseen sisältyy nimenomainen lauseke keskeisten suorituskykyindikaattoreiden seurannasta, samoin kuin arviointia ja uudelleentarkastelua koskeva lauseke, jonka mukaan Euroopan komissio tekee väliarvioinnin säädöksen vaikutuksen ja sen tuoman lisäarvon määrittämiseksi. Euroopan komissio laatii arvioinnista kertomuksen Euroopan parlamentille ja neuvostolle. Komissio voi tämän arvioinnin perusteella ehdottaa osaamiskeskuksen ja verkoston toimeksiannon uudelleentarkastelua ja laajentamista.