Euroopa Liidu
Nõukogu

Brüssel, 13. september 2018
(OR. en)

Institutsioonidevaheline dokument: 2018/0328(COD)

12104/18
ADD 5

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

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Jordi AYET PUIGARNAU, direktor
Kättesaamise kuupäev:	12. september 2018
Saaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	SWD(2018) 404 final
Teema:	KOMISJONI TALITUSTE TÖÖDOKUMENT MÕJUHINNANGU KOMMENTEERITUD KOKKUVÕTE Lisatud dokumendile: ETTEPANEK: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, millega luuakse Euroopa küberturvalisuse uurimis- ja pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik

Käesolevaga edastatakse delegatsioonidele dokument SWD(2018) 404 final.

Lisatud: SWD(2018) 404 final

EUROOPA
KOMISJON

Brüssel, 12.9.2018
SWD(2018) 404 final

KOMISJONI TALITUSTE TÖÖDOKUMENT

MÕJUHINNANGU KOMMENTEERITUD KOKKUVÕTE

Lisatud dokumendile:

ETTEPANEK: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

millega luuakse Euroopa küberturvalisuse uurimis- ja pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik

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

Kommenteeritud kokkuvõte

Mõjuhinnang järgmise ettepaneku kohta: ettepanek luua pädevuskeskuste võrgustik ning Euroopa küberturvalisuse uurimis- ja pädevuskeskus

A. Vajadus meetmete järele

Miks? Mis on lahendamist vajav probleem?

ELil ei ole siiani piisavat tehnoloogilist ja tööstuslikku võimekust, et iseseisvalt tagada oma majanduse ja elutähtsa taristu turvalisus ning jõuda küberturvalisuse valdkonnas maailmas juhtivale kohale. Käesoleva algatuse eesmärk on aidata lahendada järgmised probleemid ja nendega seotud selle olukorra põhjused.

Probleem nr 1. Ebapiisav strateegiline ja jätkusuutlik koordineerimine ning koostöö tööstusvaldkondade, küberturvalisuse teaduskogukondade ja valitsuste vahel, et kaitsta majandust, ühiskonda ja demokraatiat tipptasemel Euroopa küberturvalisuse lahenduste abil.

Probleem nr 2. Ebapiisavad investeeringud ning piiratud juurdepääs küberturvalisuse valdkonna oskusteadmistele, oskustele ja rajatistele Euroopas.

Probleem nr 3. Vähestest Euroopa küberturvalisuse teadus- ja arendustegevuse tulemustest saavad turustatavad lahendused, mis võetakse majanduses ulatuslikult kasutusele.

Neil probleemidel on mitu aluspõhjust, sealhulgas küberturvalisuse turu eri osalejate ebapiisav usaldus üksteise vastu, toimuva koostöö ja olemasolevate vahendite koondamise mehhanismide olemuslikud piirangud, kulukate küberturvalisuse taristute ning toodete ja lahenduste ühishangete raamistiku puudumine ning turu tõuke- ja tõmbemehhanismide kasutamata potentsiaal.

Mida selle algatusega loodetakse saavutada?

Algatuse eesmärk on tagada, et EL säilitab ja arendab olulist (tehnoloogilist ja tööstuslikku) võimekust tagada iseseisvalt oma digitaalmajanduse, ühiskonna ja demokraatia turvalisus ning et liikmesriigid saavad kasutada kõige kõrgemal tasemel küberturvalisuse lahendusi ja küberkaitse võimekusi. Algatuse eesmärk on ka suurendada ELi küberturvalisuse ettevõtete ülemaailmset konkurentsivõimet ja tagada, et eri sektorite Euroopa tööstustel on juurdepääs võimekusele ja ressurssidele, mida on vaja, et muuta küberturvalisus oma konkurentsieeliseks. See tuleks saavutada, töötades välja kõigi asjaomaste osalejate (avaliku sektori asutused, tööstused, nii tsiviil- kui ka kaitsesektori teaduskogukond) pikaajalise strateegilise koostöö tulemuslikud mehhanismid, koondades teadmisi ja ressursse, et tagada tipptasemel võimekus ja taristud, stimuleerides Euroopa küberturvalisuse toodete ja lahenduste ulatuslikku kasutuselevõttu eri majandusvaldkondades ja avaliku sektori poolt, toetades küberturvalisuse idufirmasid ja VKEsid ning aidates kõrvaldada küberturvalisuse oskuste nappust.

Milline on ELi tasandi meetmete lisaväärtus?

Algatus annaks lisaväärtust praegu riiklikul tasandil toimuvale tegevusele, aidates luua omavahel ühendatud ning kogu Euroopat hõlmava küberturvalisuse tööstus- ja teaduskeskkonna. See peaks soodustama sidusrühmade (sealhulgas küberturvalisuse tsiviil- ja kaitsesektori) vahelist koostööd, et kasutada parimal viisil Euroopa olemasolevaid küberturvalisuse ressursse ja eksperditeadmisi. See peaks aitama ELil ja liikmesriikidel rakendada küberturvalisuse tööstuspoliitika puhul proaktiivset, pikaajalist ja strateegilist perspektiivi, mis on laiem kui lihtsalt teadus- ja arendustegevus. See lähenemisviis peaks lisaks era- ja avaliku sektori küberturvalisuse väljakutsetele murranguliste lahenduste leidmise toetamisele aitama ka neid tulemuslikult kasutusele võtta. See võimaldab ka asjaomastel teadus- ja tööstuskogukondadel ning avaliku sektori asutustel saada juurdepääsu võtmetähtsusega võimekusele, näiteks katse- ja eksperimendirajatistele, mida liikmesriigid üksi ei saa ebapiisavate rahaliste vahendite ja töötajate tõttu sageli kasutada. See aitab ka kõrvaldada oskuste nappuse ja vältida ajude äravoolu, tagades kõige andekamatele juurdepääsu suuremahulistele Euroopa projektidele ning pakkudes seega huvitavaid erialaseid väljakutseid. Kõike eespool nimetatut peetakse vajalikuks, et Euroopat tunnistataks ülemaailmselt küberturvalisuse valdkonnas juhtiva piirkonnana.

B. Lahendused

Milliseid seadusandlikke ja mitteseadusandlikke poliitikavariante on kaalutud? Kas on olemas

eelistatud variant? Miks?

Kaalutud on mitmeid seadusandlikke ja mitteseadusandlikke poliitikavariante. Põhjalikult otsustati hinnata järgmisi variante:

1. **lähtestsenaarium** – koostööl põhinev variant – eeldab, et ELis jätkatakse praegust küberturvalisuse tööstusliku ja tehnoloogilise võimekuse suurendamise lähenemisviisi, toetades teadusuuringuid ja innovatsiooni ning nendega seotud koostöömehhanisme programmi „Euroopa horisont" alusel;
2. **variant 1:** küberturvalisuse pädevusvõrgustik koos Euroopa küberturvalisuse uurimis- ja pädevuskeskusega, millel on volitused võtta tööstustehnoloogiaid toetavaid ning teadusuuringute ja innovatsiooni valdkonna meetmeid;
3. **variant 2:** küberturvalisuse pädevusvõrgustik koos Euroopa küberturvalisuse uurimis- ja pädevuskeskusega, mis piirdub ainult teadusuuringute ja innovatsiooniga.

Varajases etapis välja arvatud variandid olid 1) variant mitte tegutseda, 2) ainult võrgustiku ja pädevuskeskuste variant ning 3) olemasoleva ameti kasutamine (ENISA, REA või INEA).

Võttes arvesse üldist kohustust, mille komisjon on käesoleva algatuse puhul juba võtnud, ning liikmesriikide olulist rolli, seisneb üksikasjalikult analüüsitud kahe poliitikavariandi peamine erinevus nende ulatuses, mis kajastub nende õiguslikus aluses: Euroopa Liidu toimimise lepingu artikli 187 alusel loodava üksuse puhul (variant 2) piirduks algatus ainult teadusuuringute ja innovatsiooni valdkonnaga ning see eeldaks üldjuhul erasektori osalejate rahalist toetust. Teisest küljest oleks kahe õigusliku alusega – Euroopa Liidu toimimise lepingu artiklid 187 ja 173 – üksusel (variant 1) laiem volitus, mis hõlmaks muu hulgas ka kasutuselevõttu ja tööstuslikku toetust ning küberkaitsega suurema koostoime loomist. See annaks olulisema rolli ka liikmesriikidele – nii haldaja kui ka küberturvalisuse tehnoloogia võimaliku hankijana.

Analüüs näitas, et variant 1 on kõige parem algatuse eesmärkide saavutamiseks, avaldab samal ajal suurimat majanduslikku, ühiskondlikku ja keskkonnamõju ning kaitseb liidu huve. Peamised argumendid selle variandi kasuks olid paindlikkus võimaldada kogukonnas ja pädevuskeskuste võrgustikus eri koostöömudeleid, et kasutada parimal viisil olemasolevaid teadmisi ja vahendeid, võime struktureerida kõigist asjakohastest sektoritest, sealhulgas kaitsesektor, pärinevate avaliku ja erasektori sidusrühmade koostööd ning võime luua tegelik küberturvalisuse tööstuspoliitika, toetades mitte ainult teadus- ja arendustegevusega, aga ka turule laskmisega seotud meetmeid. Lisaks võimaldab variant 1 suurendada sidusust, olles rakendusmehhanismiks digitaalse Euroopa programmist ja programmist „Euroopa horisont" saadava küberturvalisusega seotud rahastamise jaoks ning suurendada seoses Euroopa Kaitsefondiga küberturvalisuse tsiviil- ja kaitsemõõtme vahelist koostoimet.

Kes millist varianti toetab?

Konsultatsiooni tulemuse ja tõendite kogumise protsessi kohaselt soovivad nii tööstus- kui ka teaduskogukond selgelt mehhanismi, mis võimaldab ELi sidusat küberturvalisuse tööstuspoliitikat, mis on ulatuslikum üksnes teadus- ja arendustegevusest. Ainult nii saaks Euroopast küberturvalisuse valdkonnas maailma juhtiv piirkond. Samal ajal rõhutasid sidusrühmad, et edu eelduseks on määrata täpselt kindlaks keskuse roll võrgustiku ja asjaomaste kogukondade töö toetamisel ja lihtsustamisel ning kasutada võrgustiku puhul kaasavat ja koostööl põhinevat lähenemisviisi, et vältida uut kapseldumist. Struktuur peaks ka olema paindlik, et seda oleks võimalik kergesti kohandada, võttes arvesse küberturvalisuse keskkonna kiiret muutumist. Liikmesriigid rõhutasid kogu protsessi vältel vajadust kaasata kõik liikmesriigid ning nende olemasolevad tipptaseme- ja pädevuskeskused ning pöörata eritähelepanu tegevuse vastastikusele täiendavusele. Täpsemalt rõhutasid liikmesriigid keskuse puhul selle koordineeriva rolli olulisust võrgustiku toetamisel. Seetõttu tuleks komisjoni igasuguse algatuse puhul leida haldus- ja rakendusstruktuuride õige tasakaal ning kajastada seda, et tagada tulemuslik Euroopa koordineerimine, võttes arvesse riiklikul tasandil toimuvaid sündmusi.

C. Eelistatud poliitikavariandi mõju

Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel korral peamiste poliitikavariantide) eelised?

Eelistatud poliitikavariant võimaldab avaliku sektori asutustel ja tööstusvaldkondadel liikmesriikides vältida tõhusamalt küberohte ja reageerida neile, pakkudes turvalisemaid tooteid ja lahendusi ning võttes need ise kasutusele. See on eriti tähtis, et kaitsta juurdepääsu olulistele teenustele (näiteks transport, tervishoid, pangandus ja finantsteenused). See avaldaks ka positiivset mõju ELi konkurentsivõimele ja VKEdele, kuna see

eeldab mehhanismi loomist, mis on suuteline arendama liikmesriikide ja liidu küberturvalisuse tööstuslikku võimekust ja muutma Euroopa tipptasemel teaduse tulemuslikult turustatavateks lahendusteks, mida saaks kasutusele võtta ka eri majandusvaldkondades. See variant võimaldab koondada ressursse, et investeerida vajalikku võimekusse liikmesriikide tasandil ja arendada Euroopa ühiseid vahendeid, saavutades samal ajal mastaabisäästu. See annab tõenäoliselt VKEdele, tööstusvaldkondadele ja teadlastele parema juurdepääsu neile rajatistele, mis stimuleerib innovatsiooni ja vähendab arendusprotsessideks kuluvat aega. See vähendab ka teatavate nõudluspoolsete ettevõtjate kulusid ja aitab neil muuta küberturvalisuse oma konkurentsieeliseks. Variant võimaldab kasutada ära topeltturu võimalusi, võimaldades kaitse- ja tsiviilsektori kogukondadel teha koostööd ühiste probleemide lahendamiseks. See annab tõenäoliselt ka lisaväärtust küberturvalisuse oskuste nappuse kõrvaldamiseks võetavatele riiklikele meetmetele. ELi tasandil võimaldab see variant ka suurendada eri rahastamismehhanismide sidusust ja koostoimet.

Võidakse saavutada kaudne positiivne mõju keskkonnale, arendades konkreetseid küberturvalisuse lahendusi sektorite jaoks, millel võib olla ülisuur keskkonnamõju (näiteks tuumaelektrijaamad), aidates neil vältida seda liiki taristu vastu sooritatavatest küberrünnetest tekkivaid potentsiaalselt katastroofilisi tagajärgi.

Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel korral peamiste poliitikavariantide) kulud?

Eelistatud variandi kulud on peamiselt seotud keskuse ja riiklike koordineerimiskeskuste tegevuskuludega. Eri rahastamisprogrammide (digitaalse Euroopa programm ja programm „Euroopa horisont“) rakendamisest tekkivaid kulusid käsitletakse eraldi mõjuhinnangus.

Milline on mõju ettevõtjatele, VKEdele ja mikroettevõtjatele?

Kõige enim mõjutatud sidusrühmad on küberturvalisuse nõudlus- ja pakkumispoolsed Euroopa ettevõtjad, sealhulgas küberturvalisuse valdkonnas tegutsevad VKEd ja mikroettevõtjad. Kuigi pädevuskeskuse ja võrgustiku loomine ei sea neile regulatiivseid kohustusi, annab see võimalusi uute toodete projekteerimise käigus kulude vähendamiseks, annab neile lihtsama juurdepääsu investorite kogukonnale ning aitab hankida rahastamist, mida on vaja turustatavate lahenduste kasutuselevõtuks. VKEde ja mikroettevõtjate puhul on veelgi olulisem juurdepääs avaliku sektori rahastatavatele katse- ja eksperimendirajatistele, kuna neil puuduvad ressursid vajaliku taristu ostmiseks või selle leidmiseks turust väljapoole (ja sageli väljapoole ELi) reisimiseks. Samuti loodetakse, et see algatus avab küberturvalisuse valdkonnas tegutsevate Euroopa VKEde ja mikroettevõtjate jaoks uued turud. Lisaks sellele tagab valitud mehhanism teadus- ja tööstuskogukonna vahelise koordineerimise ning seega aitab kasutada teadlaste tegevust konkreetsete tööstuse vajaduste saavutamiseks. Tipptasemel küberturvalisuse eksperditeadmiste ja vahendite tagamine aitab kaudselt ettevõtjatel täita küberturvalisuse direktiivi nõudeid.

Kas on ette näha märkimisväärset mõju riigieelarvetele ja ametiasutustele?

Algatus aitab liikmesriikidel koordineerida riiklikul ja Euroopa tasandil vajalikku küberturvalisuse taristusse tehtavaid investeeringuid. Mehhanism aitab koondada ressursse vahendite ja taristute jaoks, mis oleksid vastasel juhul konkreetsete liikmesriikide jaoks kallimad või mida nad ei saaks endale lubada. See lähenemisviis võimaldaks mastaabisäästu ja ratsionaliseerimist. Pädevuskeskusele ja asjaomastele meetmetele antav liikmesriikide rahaline toetus peaks olema samaväärne liidu sissemaksega.

Kas on oodata muud olulist mõju?

Jah, algatusel on selge positiivne mõju, kuna see suurendab eeldatavasti märkimisväärselt liikmesriikide võimet tagada iseseisvalt oma majandusvaldkondade turvalisus, sealhulgas kaitsta elutähtsaid sektoreid, suurendada Euroopa küberturvalisuse ettevõtjate ja eri sektorite tööstusvaldkondade konkurentsivõimet, tänu millele saavad nad asjakohaselt tagada oma olemasoleva vara turvalisuse ja kavandada turvalisi innovatiivseid tooteid, vähendades turvalisusega seotud teadus- ja arendustegevuse kulusid. See peaks kokkuvõttes võimaldama ELil saada juhtivaks piirkonnaks järgmise põlvkonna digitaal- ja küberturvalisuse tehnoloogiate puhul.

D. Järelmeetmed

Millal poliitika läbi vaadatakse?

Õigusakti lisatakse sõnaselge klausel võtmetähtsusega tulemuslikkuse põhinäitajate seireks ning hindamis- ja läbivaatamisklausel, mille kohaselt korraldab Euroopa Komisjon vahehindamise, et mõõta õigusakti mõju ja selle lisaväärtust. Euroopa Komisjon esitab seejärel aruanded Euroopa Parlamendile ja nõukogule. Pärast hindamist võib komisjon teha ettepaneku pädevuskeskuse ja võrgustiku volituste läbivaatamiseks ning laiendamiseks.