Eiropas Savienības
Padome

Briselē, 2018. gada 13. septembrī
(OR. en)

12104/18
ADD 5

Starpiestāžu lieta:
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

PAVADVĒSTULE

Sūtītājs:	Direktors *Jordi AYET PUIGARNAU* kungs, Eiropas Komisijas ģenerālsekretāra vārdā
Saņemšanas datums:	2018. gada 12. septembris
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretārs *Jeppe TRANHOLM-MIKKELSEN* kungs
K-jas dok. Nr.:	SWD(2018) 404 final
Temats:	KOMISIJAS DIENESTU DARBA DOKUMENTS - IETEKMES NOVĒRTĒJUMA KOPSAVILKUMS - Pavaddokuments dokumentam - PRIEKŠLIKUMS EIROPAS PARLAMENTA UN PADOMES REGULAI, ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu

Pielikumā ir pievienots dokuments SWD(2018) 404 *final*.

Pielikumā: SWD(2018) 404 *final*

EIROPAS
KOMISIJA

Briselē, 12.9.2018.
SWD(2018) 404 final

KOMISIJAS DIENESTU DARBA DOKUMENTS

IETEKMES NOVĒRTĒJUMA KOPSAVILKUMS

Pavaddokuments dokumentam

PRIEKŠLIKUMS EIROPAS PARLAMENTA UN PADOMES REGULAI,

ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu

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

Kopsavilkuma lapa

Ietekmes novērtējums par priekšlikumu izveidot Kompetenču centru tīklu un Eiropas Kiberdrošības pētniecības un kompetenču centru

A. Rīcības nepieciešamība

Pamatojums. Risināmā problēma.

Patlaban ES joprojām trūkst pietiekamu tehnoloģisko un industriālo spēju, lai autonomi aizsargātu savu ekonomiku un kritiskās infrastruktūras, kā arī kļūtu par pasaules līderi kiberdrošības jomā. Šī iniciatīva sagatavota, lai sekmētu turpmāk izklāstīto problēmu un šādu situāciju ietekmējošo jautājumu risināšanu:

1. problēma: nepietiekams stratēģiskas un ilgtspējīgas koordinācijas līmenis, kā arī nepietiekama sadarbība starp industrijām, kiberdrošības pētniecības kopienām un valdībām, lai aizsargātu ekonomiku, sabiedrību un demokrātiju, izmantojot vadošos Eiropas kiberdrošības risinājumus;

2. problēma: nepietiekamas investīcijas un ierobežota piekļuve kiberdrošības zinātībai, prasmēm un tehniskajam nodrošinājumam visā Eiropā;

3. problēma: pārāk maz Eiropas kiberdrošības pētījumu un inovāciju rezultātu tiek izmantoti tirgojamu risinājumu izstrādē un plaši izvērsti visā ekonomikā.

Šo problēmu pamatā ir vairāki iemesli, tostarp nepietiekams uzticības līmenis starp dažādiem kiberdrošības tirgus dalībniekiem, esošajiem sadarbības un līdzekļu apkopošanas mehānismiem piemītošie trūkumi, dārgu kiberdrošības produktu / risinājumu kopēju iepirkumu satvara trūkums, kā arī neizmantots tirgus darbību veicinošu mehānismu potenciāls.

Iniciatīvas mērķi.

Šīs iniciatīvas mērķis ir nodrošināt, ka ES saglabā un attīsta būtiskākās (tehnoloģiskās un industriālās) spējas, lai spētu autonomi aizsargāt savu digitālo ekonomiku, sabiedrību un demokrātiju, kā arī pārliecināties, ka dalībvalstis gūst labumu no progresīvākajiem kiberdrošības risinājumiem un kiberaizsardzības spējām. Tāpat arī šīs iniciatīvas mērķis ir palielināt ES kiberdrošības nozares uzņēmumu globālo konkurētspēju un nodrošināt, ka Eiropā industrijām dažādās nozarēs ir pieejamas spējas un resursi, lai kiberdrošību padarītu par savas konkurētspējas priekšrocību. Šie mērķi būtu jāsasniedz, izstrādājot efektīvus mehānismus ilgtermiņa stratēģiskajai sadarbībai starp visiem iesaistītajiem dalībniekiem (publiskām iestādēm, industrijām, civilās un aizsardzības jomas pētniecības kopienām), apvienojot zināšanas un resursus, lai nodrošinātu vismodernākās spējas un infrastruktūru, sekmējot plašu Eiropas kiberdrošības produktu un risinājumu izvēršanu visas ekonomikas un publiskā sektora ietvaros, atbalstot kiberdrošības jomas jaunuzņēmumus un MVU, kā arī palīdzot novērst kiberdrošības prasmju trūkumu.

ES mēroga rīcības pievienotā vērtība.

Šī iniciatīva varētu sniegt pievienoto vērtību pašreizējiem centieniem valstu līmenī, jo palīdzētu izveidot Eiropas mēroga kiberdrošības industriālo un pētniecisko ekosistēmu. Tai jāsekmē labāka sadarbība starp attiecīgajām ieinteresētajām personām (arī kiberdrošības civilajām un aizsardzības jomām), tādējādi panākot Eiropas mēroga kiberdrošības resursu un lietpratības iespējami labāko izmantojumu. Šādam scenārijam vajadzētu arī palīdzēt ES un dalībvalstīm kiberdrošības industriālajā politikā attīstīt proaktīvu, ilgtermiņa un stratēģisku perspektīvu, kas neaprobežojas tikai ar pētniecības un inovācijas jomu. Šādai pieejai būtu ne vien jāsekmē revolucionāri risinājumi, kas ļauj risināt kiberdrošības problēmas, ar kurām sastopas gan privātais, gan publiskais sektors, bet arī jāatbalsta šādu risinājumu efektīva ieviešana praksē. Iniciatīva arī ļautu attiecīgajām pētniecības un industriālajām kopienām, kā arī publiskajām iestādēm piekļūt nozīmīgākajiem resursiem, piemēram, testēšanas un eksperimentālajam tehniskajam nodrošinājumam, kam bieži vien atsevišķa dalībvalsts nemaz nevar piekļūt, jo tai nav pietiekamu finanšu un cilvēkresursu. Nodrošinot talantīgāko speciālistu piesaistīšanu liela mēroga Eiropas projektos un tādējādi piedāvājot interesantas profesionālās izaugsmes iespējas, tā arī palīdzēs novērst prasmju trūkumu un intelektuālā darbaspēka emigrāciju. Viss iepriekšminētais arī tiek uzskatīts par nepieciešamu, lai Eiropu visā pasaulē atzītu par kiberdrošības jomas līderi.

B. Risinājumi

Apsvērtie leģislatīvie un neleģislatīvie politikas risinājumi. Vēlamais variants. Pamatojums.

Tika apsvērti vairāki leģislatīvi un neleģislatīvi politikas risinājumi. Tika veikts padziļināts novērtējums par šādiem risinājumiem:

1. **Pamatscenārijs** — sadarbības risinājums — pieņem pašreizējās pieejas turpināšanu, lai ES veidotu kiberdrošības industriālās un tehnoloģiskās spējas, atbalstot pētniecību un inovāciju, kā arī saistītos sadarbības mehānismus saskaņā ar pamatprogrammu "Apvārsnis Eiropa";
2. **1. risinājums:** Kiberdrošības kompetenču tīkls ar Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru — struktūru, kas pilnvarota veikt pasākumus, lai atbalstītu industriālās tehnoloģijas, kā arī pasākumus pētniecības un inovācijas jomā;
3. **2. risinājums:** Kiberdrošības kompetenču tīkla un Eiropas Kiberdrošības pētniecības un kompetenču centra darbība tikai pētniecības un inovācijas jomā.

Sākotnējā posmā tika atmesti šādi risinājumi: 1) neveikt nekādas darbības, 2) izmantot tikai jau pastāvošus kompetenču centrus un 3) izmantot pastāvošu aģentūru (*ENISA*, *REA* un *INEA*).

Ņemot vērā vispārējās saistības, ko Komisija jau ir uzņēmusies attiecībā uz pašreizējo iniciatīvu, kā arī ņemot vērā dalībvalstu nozīmīgo lomu, galvenā atšķirība starp abiem politikas risinājumiem, par kuriem tika veikta detalizēta analīze, ir to darbības tvērumā, kas atspoguļots to juridiskajā pamatā: struktūra, kas balstīta tikai uz LESD 187. pantu (2. risinājums), iniciatīvas darbību ierobežotu un attiecinātu tikai uz pētniecības un inovācijas jomu, kā arī normālos apstākļos paredzētu privātā sektora dalībnieku finansiālu ieguldījumu. Turpretī struktūra, kas balstīta uz divkārša juridiskā pamata — LESD 187. pantu un LESD 173. pantu (1. risinājums), nozīmētu plašākas pilnvaras, cita starpā aptverot atbalstu plašākai ieviešanai un industriālajām spējām un radot spēcīgāku sinerģiju ar kiberaizsardzību. Tādējādi tiktu arī pastiprināta dalībvalstu nozīme gan attiecībā uz to lomu pārvaldē, gan arī to lomu potenciālo kiberdrošības tehnoloģiju ieguvēju statusā.

Analīze apliecināja, ka 1. risinājums ir vispiemērotākais, lai sasniegtu iniciatīvas mērķus, vienlaikus piedāvājot visaugstāko ekonomisko, sociālo un vides ietekmi un aizsargājot Savienības intereses. Galvenie argumenti šī risinājuma labā ietver elastīgumu, kas ļautu pielietot dažādus modeļus sadarbībai ar kopienu un kompetenču centru tīklu, lai optimizētu jau apgūto zināšanu un resursu izmantošanu, iespēju strukturēt visu attiecīgo nozaru, tostarp aizsardzības nozares, publisko un privāto ieinteresēto personu sadarbību, iespēju izveidot reālu kiberdrošības industriālo politiku, atbalstot darbības, kas saistītas ne tikai ar pētniecību un izstrādi, bet arī ar ieviešanu tirgū. Visbeidzot, taču ne mazāk svarīgi, 1. risinājums ļauj arī palielināt saskaņotību, darbojoties kā īstenošanas mehānisms attiecībā uz kiberdrošības jomas finansējumu no Digitālās Eiropas programmas un pamatprogrammas "Apvārsnis Eiropa", kā arī veicinot sinerģijas starp kiberdrošības civilajām un aizsardzības dimensijām saistībā ar Eiropas Aizsardzības fondu.

Atbalsts konkrētajiem risinājumiem.

Saskaņā ar apspriešanās un pierādījumu vākšanas pasākumu rezultātiem, ja Eiropa vēlas kļūt par globālu līderi kiberdrošības jomā, gan industrijas, gan pētniecības kopienām ir redzama skaidra nepieciešamība pēc mehānisma, kas ļautu ES izveidot saskaņotu kiberdrošības industriālo politiku, kas būtu plašāka par darbībām pētniecības un izstrādes jomā. Tajā pašā laikā ieinteresētās personas uzsvēra, ka panākumu atslēga būs precīzi definēta Kompetenču centra loma, atbalstot un atvieglojot Tīkla un attiecīgo kopienu centienus, kā arī iekļaujoša un kopīga pieeja Tīklam, lai izvairītos no jaunas sadrumstalotības veidošanas. Struktūrai jābūt elastīgai, lai to varētu viegli pielāgot, ņemot vērā, ka kiberdrošība ir vide ar strauju attīstību. Visa procesa gaitā dalībvalstis uzsvēra vajadzību būt iekļaujošiem attiecībā uz visām dalībvalstīm un to esošajiem izcilības un ompetenču centriem, kā arī pievērst īpašu uzmanību darbību papildināmībai. Konkrēti attiecībā uz Kompetenču centru dalībvalstis uzsvēra tā svarīgo lomu Tīkla atbalsta koordinēšanā. Tādēļ jebkurā Komisijas iniciatīvā būs jāatrod pareizais līdzsvars starp vadības un īstenošanas struktūrām un šis līdzsvars jāatspoguļo pārvaldības un īstenošanas struktūrās, lai nodrošinātu efektīvu Eiropas koordināciju, vienlaikus ņemot vērā norises valstu līmenī.

C. Vēlamā risinājuma ietekme

Ieguvums no vēlamā risinājuma (ja nav, no galvenajiem risinājumiem).

Vēlamais risinājums ļaus dalībvalstu publiskajām iestādēm un industrijām efektīvāk novērst kiberdraudus un uz tiem reaģēt, apgādājot sevi ar drošākiem produktiem un risinājumiem. Tas ir jo īpaši svarīgi, lai aizsargātu piekļuvi būtiskiem pakalpojumiem (piemēram, transporta, veselības, banku un finanšu pakalpojumiem). Risinājumam arī būtu pozitīva ietekme uz ES konkurētspēju un MVU, jo tas paredz tāda mehānisma izveidi, kas veidotu dalībvalstu un Savienības kiberdrošības industriālās spējas un efektīvi pārveidotu Eiropas zinātnisko izcilību tirgojamos risinājumos, kurus varētu izvērst visā ekonomikā. Šis risinājums ļauj apvienot resursus, lai dalībvalstu līmenī veiktu investīcijas vajadzīgo spēju veidošanā un attīstītu Eiropas kopīgos aktīvus, vienlaikus panākot apjomradītus ietaupījumus. Tādējādi visdrīzāk palielināsies MVU, industriju un pētnieku piekļuve tādam tehniskajam nodrošinājumam, kas veicinās inovāciju un saīsinās attīstības procesus. Tas arī samazinās atsevišķu pieprasījuma puses uzņēmumu izmaksas un palīdzēs tiem pārvērst kiberdrošību par viņu konkurētspējas priekšrocību. Šis risinājums paredz izmantot divējāda lietojuma tirgus iespējas, ļaujot aizsardzības un civilajām kopienām kopīgi strādāt pie kopējām problēmām. Tas varētu arī sniegt pievienoto vērtību valstu centieniem, kas saistīti ar kiberdrošības prasmju trūkuma novēršanu. Eiropas Savienības līmenī šis risinājums ļauj arī uzlabot saskaņotību un sinerģijas starp dažādiem finansēšanas mehānismiem.

Netiešu pozitīvu ietekmi uz vidi varētu panākt, izstrādājot konkrētus kiberdrošības risinājumus nozarēm, kurām ir potenciāli liela ietekme uz vidi (piemēram, kodolelektrostacijām), tādējādi palīdzot izvairīties no potenciāli postošām sekām, ko var radīt kiberuzbrukumi šāda veida infrastruktūrai.

Vēlamā risinājuma izmaksas (ja tādas nav, galveno risinājumu izmaksas).

Izdevumi, kas saistīti ar vēlamo risinājumu, galvenokārt ir saistīti ar Kompetenču centra un valstu koordinācijas centru funkcionēšanas izmaksām. Attiecībā uz izmaksām, kas saistītas ar dažādu finansēšanas programmu (Digitālās Eiropas programmas un pamatprogrammas "Apvārsnis Eiropa") īstenošanu, jāveic atsevišķi ietekmes novērtējumi.

Ietekme uz uzņēmumiem, MVU un mikrouzņēmumiem.

Visvairāk tiks ietekmētas ieinteresēto personu grupas no Eiropas uzņēmumiem gan kiberdrošības nozares pieprasījuma, gan piedāvājuma pusē, tostarp MVU un mikrouzņēmumiem, kas darbojas kiberdrošības jomā. Lai arī Kompetenču centra un Tīkla izveide tiem neuzliek reglamentējošas saistības, tā pavērs iespējas jaunu produktu izstrādes izmaksu samazināšanā un palīdzēs tiem vieglāk piekļūt investoru kopienai un piesaistīt nepieciešamo finansējumu tirgojamu risinājumu ieviešanai. Attiecībā uz MVU un mikrouzņēmumiem pieejamība publiski finansētām izmēģinājumu un eksperimentu sistēmām ir vēl jo svarīgāka, jo tiem trūkst līdzekļu, lai iegādātos nepieciešamo infrastruktūru vai ceļotu ārpus to tirgus (bieži vien arī ārpus ES) infrastruktūras meklējumos. Tāpat tiek cerēts, ka šī iniciatīva pavērs jaunus tirgus Eiropas MVU un mikrouzņēmumiem, kas aktīvi darbojas kiberdrošības jomā. Turklāt izvēlētais mehānisms nodrošinās pētniecības un industrijas koordināciju un tādējādi novirzīs pētniecības centienus konkrētām industriālajām vajadzībām. Jaunākās lietpratības un rīku nodrošināšana kiberdrošības jomā netieši atbalstīs uzņēmējus TID direktīvas ievērošanā.

Nozīmīga ietekme uz valstu budžetiem un valsts pārvaldi.

Iniciatīva ļaus dalībvalstīm koordinēt investīcijas nepieciešamajās kiberdrošības infrastruktūrās valstu un Eiropas līmenī. Šis mehānisms ļaus apvienot resursus rīkiem un infrastruktūrām, kas citādi būtu dārgāki vai kurus atsevišķas dalībvalstis nevarētu atļauties. Šāda pieeja nodrošinātu apjomradītus ietaupījumus un racionalizāciju. Dalībvalstu finansiālajam ieguldījumam Kompetenču centrā un saistītajās darbībās jābūt proporcionālam attiecībā pret Savienības ieguldījumu.

Cita nozīmīga ietekme.

Iniciatīvai ir skaidra pozitīva ietekme, jo tā var būtiski palielināt dalībvalstu spēju autonomi aizsargāt to ekonomiku, tai skaitā, aizsargāt kritiskās nozares, palielinot Eiropas kiberdrošības jomas uzņēmumu, kā arī industriju konkurētspēju dažādās nozarēs, lai tās spētu pienācīgi aizsargāt esošos aktīvus un izstrādāt drošus, novatoriskus produktus, vienlaikus samazinot ar drošību saistītās pētniecības un izstrādes izmaksas. Tas galu galā ļaus ES kļūt par līderi nākamās paaudzes digitālo un kiberaizsardzības tehnoloģiju jomā.

D. Turpmākie pasākumi
Politikas pārskatīšanas termiņš.
Juridiskajā instrumentā tiks iekļauta īpaša klauzula, lai uzraudzītu galvenos darbības rādītājus, kā arī novērtēšanas un pārskatīšanas klauzula, saskaņā ar kuru Eiropas Komisija veiks starpposma novērtējumu, lai izvērtētu instrumenta ietekmi un tā pievienoto vērtību. Eiropas Komisija pēc tam ziņos Eiropas Parlamentam un Padomei. Pēc šā novērtējuma Komisija var ierosināt pārskatīt un paplašināt Kompetenču centra un Tīkla pilnvaras.