Europos Sąjungos
Taryba

Briuselis, 2018 m. rugsėjo 13 d.
(OR. en)

12104/18
ADD 5

Tarpinstitucinė byla:
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

PRIDEDAMAS PRANEŠIMAS

nuo:	Europos Komisijos generalinio sekretoriaus, kurio vardu pasirašo direktorius Jordi AYET PUIGARNAU
gavimo data:	2018 m. rugsėjo 12 d.
kam:	Europos Sąjungos Tarybos generaliniam sekretoriui Jeppe TRANHOLMUI-MIKKELSENUI
Komisijos dok. Nr.:	SWD(2018) 404 final
Dalykas:	KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS „POVEIKIO VERTINIMO SANTRAUKA“ pridedamas prie PASIŪLYMO DĖL EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas

Delegacijoms pridedamas dokumentas SWD(2018) 404 final.

Pridedama: SWD(2018) 404 final

EUROPOS
KOMISIJA

Briuselis, 2018 09 12
SWD(2018) 404 final

KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS

POVEIKIO VERTINIMO SANTRAUKA

pridedamas prie

PASIŪLYMO DĖL EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO

kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas

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

Santraukos lentelė

Poveikio vertinimas Pasiūlymas sukurti Kompetencijos centrų tinklą ir Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centrą

A. Būtinybė imtis veiksmų

Kodėl? Kokia problema sprendžiama?

Šiuo metu ES vis dar trūksta technologinių ir pramonės pajėgumų, kad ji galėtų savarankiškai apsaugoti savo ekonomiką bei ypatingos svarbos infrastruktūrą ir tapti pasauline lydere kibernetinio saugumo srityje. Šia iniciatyva siekiama padėti spręsti tokias su esama situacija susijusias problemas ir veiksnius:

1 problema: nepakankamas strateginio ir tvaraus pramonės įmonių, kibernetinio saugumo mokslinių tyrimų bendruomenių ir vyriausybių veiklos koordinavimo ir bendradarbiavimo lygis siekiant apsaugoti ekonomiką, visuomenę ir demokratiją, pasitelkus pažangiausius Europos sukurtus kibernetinio saugumo sprendimus;

2 problema: mažos apimties investicijos ir ribotos galimybės naudotis kibernetinio saugumo praktine patirtimi, įgūdžiais ir infrastruktūra visoje Europoje;

3 problema: per mažai Europos kibernetinio saugumo tyrimų ir inovacijų rezultatų paversta tinkamais parduoti sprendimais ir plačiai naudojama visoje ekonomikoje.

Šias problemas lemia tam tikri veiksniai, įskaitant nepakankamą skirtingų kibernetinių saugumo rinkos dalyvių tarpusavio pasitikėjimą, būdingus esamų bendradarbiavimo ir lėšų telkimo mechanizmų ribotumus, brangios kibernetinio saugumo infrastruktūros ir kibernetinio saugumo produktų ir (arba) sprendimų bendrų viešųjų pirkimų sistemos nebuvimą, taip pat neišnaudotas rinkos skatinimo mechanizmų galimybes.

Ko siekiama šia iniciatyva?

Šia iniciatyva siekiama užtikrinti ES esminių (technologinių ir pramonės) pajėgumų išsaugojimą ir kūrimą, kad ji galėtų savarankiškai apsaugoti savo skaitmeninę ekonomiką, visuomenę ir demokratiją ir kad valstybės narės galėtų pasinaudoti pažangiausiais kibernetinio saugumo sprendimais ir kibernetinės gynybos pajėgumais. Iniciatyva taip pat siekiama padidinti ES kibernetinio saugumo bendrovių konkurencingumą pasaulyje ir suteikti skirtinguose sektoriuose veikiančioms Europos pramonės įmonėms galimybę naudotis pajėgumais ir ištekliais, kad kibernetinis saugumas taptų jų konkurenciniu pranašumu. Šių tikslų turėtų būti siekiama kuriant veiksmingus ilgalaikio strateginio visų susijusių dalyvių (valdžios institucijų, pramonės įmonių, mokslinių tyrimų bendruomenės civiliniame ir gynybos sektoriuje) bendradarbiavimo mechanizmus, telkiant žinias ir išteklius pažangiausiems pajėgumams ir infrastruktūrai sukurti, skatinant plataus masto Europos kibernetinio saugumo produktų ir sprendimų diegimą ekonomikoje ir viešajame sektoriuje, remiant startuolius ir MVĮ, veikiančius kibernetinio saugumo srityje, taip pat padedant užpildyti kibernetinio saugumo įgūdžių spragas.

Kokia būtų papildoma ES lygmens veiksmų nauda?

Iniciatyva prisidėtų prie dabartinių pastangų nacionaliniu lygmeniu, nes padėtų sukurti tarpusavyje susijusią visos Europos masto kibernetinio saugumo pramonės ir mokslinių tyrimų ekosistemą. Ji turėtų paskatinti geresnį atitinkamų suinteresuotųjų šalių (įskaitant kibernetinio saugumo civilinį ir gynybos sektorius) bendradarbiavimą, kad būtų galima kuo geriau naudotis esamais po visą Europą išsibarsčiusiais kibernetinio saugumo ištekliais ir patirtimi šioje srityje. Ji turėtų padėti ES ir valstybėms narėms taikyti iniciatyvų, ilgalaikį ir strateginį požiūrį į kibernetinio saugumo pramonės politiką, apimantį ne tik mokslinius tyrimus ir technologinę plėtrą. Šis metodas turėtų ne tik padėti sukurti proveržio sprendimus, padėsiančius išspręsti kibernetinio saugumo problemas, su kuriomis susiduria viešasis ir privatus sektoriai, bet ir paremtų veiksmingą šių sprendimų įdiegimą. Tai taip pat sudarytų sąlygas atitinkamoms mokslinių tyrimų ir pramonės bendruomenės bei valdžios institucijoms naudotis svarbiausiais pajėgumais, pvz., bandymų ir eksperimentų infrastruktūra, kuriais pavienės valstybės narės dažnai negali pasinaudoti, nes neturi pakankamai finansinių ir žmogiškųjų išteklių. Iniciatyva taip pat padės išspręsti gebėjimų trūkumo problemą ir išvengti protų nutekėjimo, nes geriausiems talentams bus užtikrinta galimybė dalyvauti didelio masto Europos projektuose ir taip suteikti jiems įdomių profesinių iššūkių. Visi pirmiau išdėstyti argumentai laikomi būtinais, kad Europa būtų pripažįstama kaip lyderė kibernetinio saugumo srityje.

B. Sprendimai

Kokios su teisėkūra susijusios ir nesusijusios politikos galimybės apsvarstytos? Ar viena iš politikos galimybių pasirinkta kaip tinkamiausia? Kodėl?

Apsvarstytos įvairios tiek teisėkūros, tiek ne teisėkūros pobūdžio politikos galimybės. Buvo atliktas išsamus toliau išvardytų galimybių vertinimas:

1. Bendradarbiavimo varianto **atskaitos scenarijuje** perimtas dabartinis požiūris į kibernetinio saugumo pramonės ir technologinių pajėgumų kūrimą ES, remiant mokslinius tyrimus ir inovacijas bei susijusius bendradarbiavimo mechanizmus pagal programą „Europos horizontas";
2. **1 galimybė:** Kibernetinio saugumo kompetencijos centrų tinklo ir Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centro organizacijai suteikiami įgaliojimai įgyvendinti priemones, kuriomis būtų remiamos pramonės technologijos, taip pat priemones mokslinių tyrimų ir inovacijų srityje;
3. **2 galimybė:** Kibernetinio saugumo kompetencijos centrų tinklo ir Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centro veikla sutelkta tik į mokslinius tyrimus ir inovacijas.

Ankstyvuosiuose etapuose atmestos galimybės: 1) galimybė nesiimti jokių veiksmų, 2) galimybė naudoti tik esamų kompetencijos centrų tinklą ir 3) galimybė naudotis jau veikiančia agentūra (Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA), Mokslinių tyrimų vykdomąja įstaiga (REA) arba Inovacijų ir tinklų programų vykdomąja įstaiga (INEA)).

Atsižvelgiant į bendruosius Komisijos prisiimtus įsipareigojimus dėl šios iniciatyvos, taip pat atsižvelgiant į svarbų valstybių narių vaidmenį ją įgyvendinant, pagrindinis dviejų išsamiai nagrinėtų galimybių skirtumas yra jų taikymo sritis, kaip nurodyta jų teisiniame pagrindime: įsteigus subjektą remiantis tik SESV 187 straipsniu (2 galimybė), iniciatyva būtų apribota mokslinių tyrimų ir inovacijų sritimi, kuri paprastai finansuojama privataus sektoriaus dalyvių lėšomis. Kita vertus, įsteigus subjektą remiantis dvigubu teisiniu pagrindu, t. y. SESV 187 straipsniu ir 173 straipsniu (1 galimybė), jam būtų suteikti didesnio masto įgaliojimai, įskaitant, be kita ko, diegimą rinkoje ir pramonės paramą bei sinergijų su kibernetine gynyba stiprinimą. Tokiu atveju valstybėms narėms taip pat būtų suteiktas svarbesnis vaidmuo tiek vykdant valdymo dalyvio, tiek galimo kibernetinio saugumo technologijų pirkėjo funkcijas.

Atlikus analizę buvo padaryta išvada, kad 1 galimybė geriausiai tinka iniciatyvos tikslams pasiekti, užtikrinant aukščiausią ekonominį, socialinį ir aplinkosauginį poveikį bei apsaugant Sąjungos interesus. Tarp pagrindinių šią galimybę remiančių argumentų paminėtini lankstumas sudarant sąlygas plėtoti skirtingus bendradarbiavimo su bendruomene ir kompetencijos centrų tinklu modelius, siekiant optimizuoti esamų žinių ir išteklių naudojimą; gebėjimas struktūrizuoti viešųjų ir privačių suinteresuotųjų šalių, atstovaujančių visiems susijusiems sektoriams, įskaitant gynybą, bendradarbiavimą; galimybė kurti tikrą kibernetinio saugumo pramonės politiką remiant veiklą, susijusią ne tik su moksliniais tyrimais ir technologine plėtra, bet ir su diegimu rinkoje. Galiausiai, pasirinkus 1 galimybę, galima padidinti darną ir įgalinti kibernetinio saugumo finansavimo srautų įgyvendinimo mechanizmą pagal Skaitmeninės Europos programą ir programą „Europos horizontas", kartu skatinant karinių ir civilinių kibernetinio saugumo pastangų sinergiją, susijusią su Europos gynybos fondu.

Kas kuriai galimybei pritaria?

Remiantis konsultacijų ir įrodymų rinkimo proceso rezultatais, akivaizdu, kad tiek pramonės, tiek mokslinių tyrimų bendruomenėms reikalingas mechanizmas, kuris sudarytų sąlygas ES sukurti nuoseklią kibernetinio saugumo pramonės politiką, apimančią ne tik mokslinių tyrimų ir technologinės plėtros veiklą, kad Europa galėtų tapti pasauline lydere kibernetinio saugumo srityje. Kartu suinteresuotosios šalys pabrėžė, kad svarbiausias sėkmės veiksnys yra tinkamai apibrėžtas Centro vaidmuo remiant ir palengvinant Tinklo bei atitinkamų bendruomenių pastangas, taip pat įtraukus, bendradarbiavimu pagrįstas požiūris į tinklą, siekiant išvengti naujų duomenų kūrimo. Struktūra taip pat turėtų būti lanksti ir lengvai pritaikoma, atsižvelgiant į sparčiai kintančią kibernetinio saugumo aplinką. Dalyvaudamos procese valstybės narės pabrėžė būtinybę įtraukti visas valstybes nares ir jų esamus pažangiosios patirties ir kompetencijos centrus bei ypatingą dėmesį skirti papildomumui. Konkrečiai dėl Centro valstybės narės pabrėžė, kad svarbu koordinuoti jo vaidmenį remiant tinklą. Todėl įgyvendinant bet kokią Komisijos iniciatyvą būtina užtikrinti tinkamą valdymo ir įgyvendinimo struktūrų pusiausvyrą ir atspindėti šią pusiausvyrą valdymo ir įgyvendinimo struktūrose, siekiant užtikrinti veiksmingą Europos koordinavimą, kartu atsižvelgiant į pokyčius nacionaliniu lygmeniu.

C. Tinkamiausios galimybės poveikis

Kokie būtų tinkamiausios galimybės (jei jos nėra – pagrindinių galimybių) pranašumai?

Tinkamiausia galimybe visų valstybių narių valdžios institucijoms ir pramonės įmonėms bus suteikta galimybė veiksmingiau užkirsti kelią kibernetinėms grėsmėms ir į jas reaguoti, siūlant saugesnius produktus ir sprendimus ir jais aprūpinant. Tai ypač svarbu siekiant užtikrinti galimybę naudotis pagrindinėmis paslaugomis (pvz., transporto, sveikatos apsaugos, bankų ir finansinėmis paslaugomis). Ši galimybė taip pat turėtų teigiamą poveikį ES konkurencingumui ir MVĮ, nes pagal ją numatoma kurti mechanizmą, kuriuo būtų galima stiprinti valstybių narių ir Sąjungos kibernetinio saugumo pramoninius pajėgumus, o Europos mokslo pažangiąją patirtį sėkmingai paversti rinkai tinkamais sprendimais, kurie galėtų būti diegiami visoje ekonomikoje. Šia galimybe sudaromos sąlygos sutelkti išteklius investicijoms į būtinus pajėgumus valstybių narių lygmeniu ir plėtoti Europos bendrąjį turtą, kartu pasinaudojant masto ekonomija. Dėl to MVĮ, pramonės įmonėms ir tyrėjams greičiausiai galėtų būti suteikta daugiau galimybių naudotis tokia infrastruktūra ir taip būtų skatinamos inovacijos ir trumpinami diegimo procesai. Taip pat sumažės kai kurių paklausos srities įmonių išlaidos, o kibernetinis saugumas taps jų konkurenciniu pranašumu. Pasirinkus šią galimybę, bus galima pasinaudoti dvejopo naudojimo prekių rinkos galimybėmis, sudarius sąlygas gynybos ir civilinėms bendruomenėms kartu spręsti bendras problemas. Taip pat bus remiamos pastangos nacionaliniu lygmeniu užpildyti kibernetinio saugumo įgūdžių spragas. ES lygmeniu ši galimybė taip pat sudarys sąlygas pagerinti skirtingų finansavimo mechanizmų darną ir sinergiją.

Netiesioginis teigiamas poveikis aplinkai galėtų būti pasiektas rengiant specialius kibernetinio saugumo sprendimus sektoriams, kurie gali turėti didžiulį poveikį aplinkai (pvz., branduolinėms elektrinėms), padedant išvengti potencialiai niokojančių kibernetinio saugumo išpuolių pasekmių šiai infrastruktūrai.

Kokios būtų tinkamiausios galimybės (jei jos nėra – pagrindinių galimybių) įgyvendinimo išlaidos?

Su tinkamiausia galimybe siejamos išlaidos daugiausiai susijusios su Centro ir Nacionalinių koordinavimo centrų veikimu. Skirtingų finansavimo programų (Skaitmeninės Europos programos ir programos „Europos horizontas“) įgyvendinimo išlaidos bus nagrinėjamos atskiru poveikio vertinimu.

Koks bus poveikis verslui, MVĮ ir labai mažoms įmonėms?

Tarp suinteresuotųjų šalių grupių didžiausią poveikį pajus tiek kibernetinio saugumo paklausos, tiek pasiūlos srities subjektai – Europos bendrovės, įskaitant VMĮ ir labai mažas įmones, vykdančios veiklą kibernetinio saugumo srityje. Kadangi dėl Kompetencijos centro ir Tinklo įsteigimo nenumatoma jokių naujų reglamentavimo įsipareigojimų įmonėms, atsiras naujų išlaidų mažinimo galimybių kuriant naujus produktus; jos taip pat galės paprasčiau pasiekti investuotojų bendruomenę ir pritraukti reikalingą finansavimą, kad galėtų įdiegti tinkamus sprendimus rinkoje. MVĮ ir labai mažoms įmonėms dar svarbiau gauti galimybę naudotis viešai finansuojamomis bandymų ir eksperimentų infrastruktūra, kadangi joms trūksta išteklių įsigyti tokią infrastruktūrą ar pasinaudoti ja už savo rinkos ribų (dažnai – už ES ribų). Taip pat tikimasi, kad įgyvendinus šią iniciatyvą Europos MVĮ ir labai mažoms įmonėms, veikiančioms kibernetinio saugumo srityje, bus atvertos naujos rinkos. Be to, pasirinktu mechanizmu bus užtikrintas koordinavimas tarp mokslinių tyrimų ir pramonės, taip formuojant mokslinių tyrimų pastangas pagal konkrečius pramonės poreikius. Galimybė naudotis pažangiausia kibernetinio saugumo patirtimi ir priemonėmis netiesiogiai padės ekonominės veiklos vykdytojams siekti atitikties pagal TIS direktyvą.

Ar bus didelis poveikis nacionaliniams biudžetams ir administravimo subjektams?

Įgyvendinus iniciatyvą valstybės narės galės koordinuoti investicijas į reikiamą kibernetinio saugumo infrastruktūrą nacionaliniu ir Europos lygmenimis. Mechanizmas sudarys sąlygas sutelkti išteklius, reikalingus priemonėms ir infrastruktūrai, kurios priešingu atveju būtų per brangios ar nepasiekiamos pavienėms valstybėms narėms, įsigyti. Tokiu požiūriu įgalinama masto ekonomija ir racionalizavimas. Valstybių narių finansinis įnašas į Kompetencijos centrą ir susijusias veiklas turėtų būti proporcingas Sąjungos įnašui.

Ar bus dar koks nors didelis poveikis?

Taip, iniciatyva turės aiškų teigiamą poveikį, kadangi ji greičiausiai labai padidins valstybių narių pajėgumus savarankiškai apsaugoti savo ekonomikas, įskaitant ypatingos svarbos sektorių apsaugą, Europos kibernetinio saugumo įmonių bei kituose sektoriuose veikiančių pramonės įmonių konkurencingumo didinimą, nes jos galės tinkamai apsaugoti turimą turtą ir kurti saugius inovatyvius produktus, kartu mažindamos su MTTP susijusias išlaidas. Todėl galiausiai ES taps naujos kartos skaitmeninių ir kibernetinio saugumo technologijų lydere.

D. Tolesni veiksmai
Kada politika bus persvarstoma?
Į teisinę priemonę bus įtraukta išsami nuostata, skirta pagrindiniams veiklos rodikliams stebėti, taip pat vertinimo ir peržiūros nuostata, pagal kurią Europos Komisija atliks tarpinį vertinimą, kad galėtų įvertinti priemonės poveikį ir jos pridėtinę vertę. Vėliau Europos Komisija pateiks ataskaitą Europos Parlamentui ir Tarybai. Po atlikto vertinimo Komisija gali pasiūlyti persvarstyti ir išplėsti Kompetencijos centro ir Tinklo įgaliojimus.