Vijeće
Europske unije

Bruxelles, 13. rujna 2018.
(OR. en)

12104/18
ADD 5

Međuinstitucijski predmet:
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

POPRATNA BILJEŠKA

Od:	Glavni tajnik Europske komisije, potpisao g. Jordi AYET PUIGARNAU, direktor
Datum primitka:	12. rujna 2018.
Za:	g. Jeppe TRANHOLM-MIKKELSEN, glavni tajnik Vijeća Europske unije
Br. dok. Kom.:	SWD(2018) 404 final
Predmet:	RADNI DOKUMENT SLUŽBI KOMISIJE SAŽETAK PROCJENE UČINKA priložen dokumentu PRIJEDLOG UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara

Za delegacije se u prilogu nalazi dokument SWD(2018) 404 final.

Priloženo: SWD(2018) 404 final

EUROPSKA
KOMISIJA

Bruxelles, 12.9.2018.
SWD(2018) 404 final

RADNI DOKUMENT SLUŽBI KOMISIJE

SAŽETAK PROCJENE UČINKA

priložen dokumentu

PRIJEDLOG UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara

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

Sažetak

Procjena učinka: Prijedloga o stvaranju Mreže centara za stručnost i Europskog centra za istraživanje i stručnost u području kibersigurnosti

A. Potreba za djelovanjem

Zašto? O kakvom je problemu riječ?

EU danas i dalje nema dostatne tehnološke i industrijske kapacitete da može neovisno zaštititi svoje gospodarstvo i ključne infrastrukture te postati globalni predvodnik u području kibersigurnosti. Ovom inicijativom nastoji se pridonijeti rješavanju sljedećih problema i uzroka koji pridonose takvom stanju:

problem 1.: nedostatna razina strateške i održive koordinacije i suradnje među industrijama, istraživačkim zajednicama u području kibersigurnosti i vladama u cilju zaštite gospodarstva, društva i demokracije s najsuvremenijim europskim rješenjima u području kibersigurnosti;

problem 2.: nedostatna ulaganja i ograničeni pristup znanju i iskustvu u području kibersigurnosti te vještinama i infrastrukturi u cijeloj Europi;

problem 3.: mali broj rezultata istraživanja i inovacija u području kibersigurnosti u Europi pretvara se u rješenja koja se mogu stavljati na tržište i primjenjuje u čitavom gospodarstvu.

Postoji niz uzroka tih problema, uključujući nedostatnu razinu povjerenja među dionicima na tržištu kibersigurnosti, specifična ograničenja u postojećoj suradnji i mehanizmima udruživanja sredstava, nepostojanje okvira za zajedničku nabavu skupe infrastrukture za kibersigurnost i proizvoda/rješenja za kibersigurnost i neiskorišteni potencijal tržišnih mehanizama odbijanja i privlačenja.

Što se nastoji postići ovom inicijativom?

Inicijativom se nastoji osigurati da EU zadrži i razvije osnovne (tehnološke i industrijske) kapacitete za neovisnu zaštitu svojeg digitalnog gospodarstva, društva i demokracije i da države članice imaju na raspolaganju najnaprednija rješenja za kibersigurnost i sposobnosti za kiberobranu. Inicijativom se nastoji povećati i globalna konkurentnost poduzeća EU-a u području kibersigurnosti i osigurati da europske industrije u različitim sektorima imaju pristup kapacitetima i sredstvima koja će im omogućiti da kibersigurnost pretvore u svoju konkurentnu prednost. To bi trebalo postići razvojem djelotvornih mehanizama za dugoročnu stratešku suradnju svih relevantnih dionika (tijela javne vlasti, industrija, istraživačke zajednice iz civilnog i obrambenog područja), udruživanjem znanja i sredstava za pružanje najnaprednijih sposobnosti i infrastruktura, poticanjem široke primjene europskih proizvoda i rješenja za kibersigurnost u cijelom gospodarstvu i javnom sektoru, podupiranjem novih poduzeća i MSP-ova u području kibersigurnosti i pomaganjem u rješavanju problema manjka vještina u području kibersigurnosti.

Koja je dodana vrijednost djelovanja na razini EU-a?

inicijativom bi se mogla dodati vrijednost trenutačnim naporima na nacionalnoj razini jer bi se pridonijelo stvaranju povezanog europskog ekosustava kibersigurnosti. Potaknula bi se bolja suradnja među relevantnim dionicima (među ostalim između civilnog i obrambenog sektora u području kibersigurnosti) kako bi se najbolje iskoristili postojeći resursi u području kibersigurnosti, a znanje se širilo u cijeloj Europi. Pridonijelo bi se tome da EU i države članice prihvate proaktivnu, dugoročniju i stratešku perspektivu industrijske politike o kibersigurnosti koja ne uključuje samo istraživanje i razvoj. Tim bi se pristupom trebalo omogućiti osmišljavanje revolucionarnih rješenja za probleme u području kibersigurnosti s kojima se suočavaju privatni i javni sektor te poduprijeti učinkovita primjena tih rješenja. Time će se relevantnim istraživačkim i industrijskim zajednicama te tijelima javne vlasti omogućiti pristup ključnim kapacitetima, primjerice infrastrukturi za testiranje i eksperimentiranje koja često nije dostupna pojedinim državama članicama zbog nedovoljnih financijskih i ljudskih resursa. Pridonijet će i rješavanju nedostatka vještina i sprječavanju odljeva mozgova tako što će najvećim talentima osigurati pristup velikim europskim projektima i time im omogućiti zanimljive profesionalne izazove. Sve se navedeno smatra nužnim da bi Europa mogla biti globalno priznata kao predvodnica u području kibersigurnosti.

B. Rješenja

Koje su se zakonodavne i nezakonodavne opcije politika razmatrale? Daje li se prednost određenoj opciji? Zašto?

Razmotrene su brojne opcije politika, zakonodavne i nezakonodavne. Sljedeće opcije zadržane su radi podrobnije procjene:

1. **osnovni scenarij** – suradnička opcija – pretpostavlja nastavak trenutačnog pristupa izgradnji industrijskih i tehnoloških kapaciteta u području kibersigurnosti u EU-u podupiranjem istraživanja i inovacija i povezanih mehanizama suradnje u okviru programa Obzor Europa;
2. **1. opcija:** Mreža za stručnost u području kibersigurnosti s Europskim centrom za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja koji imaju ovlasti provoditi mjere za podupiranje industrijskih tehnologija i u području istraživanja i inovacija;
3. **2. opcija:** Mreža za stručnost u području kibersigurnosti s Europskim centrom za istraživanje i stručnost u području kibersigurnosti koji su ograničeni samo na aktivnosti istraživanja i inovacija.

U ranoj fazi odbačene su sljedeće opcije 1) nedjelovanje; 2) mreža koja se sastoji samo od postojećih centara za stručnost i 3) uporaba postojeće agencije (ENISA, REA ili INEA).

Uzimajući u obzir opću obvezu koju je Komisija već preuzela u pogledu ove inicijative te s obzirom na važnu ulogu koju će imati države članice, glavna razlika između dviju podrobno analiziranih opcija politika jest u njihovu području primjene koje se temelji na njihovoj pravnoj osnovi: subjektom koji se temelji samo na članku 187. UFEU-a (2. opcija) inicijativa bi se ograničila na područje istraživanja i inovacija i obično bi pretpostavljala financijski doprinos privatnih dionika. S druge strane, subjekt utemeljen na dvostrukoj pravnoj osnovi, odnosno na članku 187. UFEU-a i članku 173. UFEU-a (1. opcija), značio bi širi mandat koji bi, među ostalim, uključivao i primjenu i industrijsku potporu te stvaranje snažnije sinergije s kiberobranom. Povećala bi se i uloga država članica, u pogledu njihove uloge u upravljanju i njihove uloge kao mogućih dobavljača tehnologije za kibersigurnost.

Analiza je pokazala da je 1. opcija najprikladnija za ostvarenje ciljeva inicijative te da se njome istodobno ostvaruje najveći gospodarski, društveni i okolišni učinak i zaštita interesa Unije. Glavni argumenti u korist te opcije uključivali su fleksibilnost omogućivanja različitih modela suradnje sa zajednicom i mrežom centara za stručnost kako bi se najbolje moglo iskoristiti postojeće znanje i sredstva, mogućnost strukturiranja suradnje javnih i privatnih dionika iz svih relevantnih sektora, među ostalim obrane, mogućnost stvaranja stvarne industrijske politike kibersigurnosti podupiranjem aktivnosti koje nisu povezane samo s istraživanjem i razvojem već i s primjenom na tržištu. I konačno, 1. opcija omogućuje i povećanje dosljednosti jer djeluje kao provedbeni mehanizam za financijska sredstva za kibersigurnost iz programa Digitalna Europa i Obzor Europa te jačanje sinergije između civilne i obrambene dimenzije kibersigurnosti u odnosu na Europski fond za obranu.

Tko podržava koju opciju?

Na temelju rezultata savjetovanja i postupaka prikupljanja dokaza može se zaključiti da u industrijskoj i istraživačkoj zajednici postoji nedvojbena potražnja za mehanizmom kojim će se EU-u omogućiti da posjeduje dosljednu industrijsku politiku u području kibersigurnosti koja ne obuhvaća samo aktivnosti istraživanja i razvoja, čime će se omogućiti da Europa postane globalni predvodnik u području kibersigurnosti. Dionici su istodobno istaknuli da će ključ uspjeha biti dobro definirana uloga Centra koja će uključivati zadaće podupiranja i olakšavanja napora Mreže i relevantnih zajednica i uključiv, suradnički pristup mreži kako bi se izbjeglo stvaranje novog silosa. Struktura bi trebala biti fleksibilna tako da se može jednostavno prilagođavati budući da je kibersigurnost okruženje koje se brzo razvija. Tijekom tog postupka države članice istaknule su da mora uključivati sve države članice i njihove postojeće centre izvrsnosti i stručnosti te da posebnu pozornost treba posvetiti komplementarnosti djelovanja. Države članice su, posebno u pogledu Centra, istaknule važnost njegove koordinacijske uloge u podupiranju mreže. Stoga će se u svakoj inicijativi Komisije morati pronaći odgovarajuća ravnoteža između upravljačke i provedbene strukture i ta će se ravnoteža morati uzeti u obzir u upravljačkim i provedbenim strukturama kako bi se osigurala djelotvorna koordinacija na europskoj razini i istodobno uzele u obzir promjene na nacionalnoj razini.

C. Učinci opcije kojoj se daje prednost

Koje su koristi opcije kojoj se daje prednost (ako takve opcije nema, navesti koristi glavnih opcija)?

Opcijom kojoj se daje prednost omogućit će se tijelima javne vlasti i industrijama u svim državama članicama da učinkovitije sprječavaju kiberprijetnje i odgovaraju na njih jer će moći ponuditi više sigurnih proizvoda i rješenja i njima se opremiti. To je posebno važno za zaštitu pristupa osnovnim uslugama (npr. promet, zdravstvo, bankarstvo i financijske usluge). Ona bi pozitivno utjecala i na konkurentnost EU-a i na MSP-ove jer pretpostavlja stvaranje mehanizma kojim se mogu izgraditi industrijski kapaciteti država članica i Unije u području kibersigurnosti i europska znanstvena izvrsnost djelotvorno pretvoriti u utrživa rješenja koja se mogu primjenjivati u čitavom gospodarstvu. Tom seopcijom omogućuje udruživanje sredstava za ulaganje u nužne kapacitete na razini država članica i za razvoj europske zajedničke imovine uz istodobno ostvarivanje ekonomija razmjera. Time će se vjerojatno povećati pristup MSP-ova, industrija i istraživača takvim objektima, što će potaknuti inovacije i zbog čega će se skratiti razvojni postupci. Na taj način smanjit će se troškovi nekih poduzeća na strani potražnje i pomoći će im se da kibersigurnost pretvore u svoju konkurentnu prednost. Tom se opcijom omogućuje iskorištavanje prilika tržišta za dvojnu namjenu te obrambenoj i civilnoj zajednici da se zajedno suočavaju s izazovima. Vjerojatno će dodati vrijednost i nacionalnim naporima usmjerenima na uklanjanje manjka vještina u području kibersigurnosti. Na razini EU-a tom se opcijom omogućuje poboljšanje dosljednosti i sinergije među različitim financijskim instrumentima.

Neizravni pozitivni utjecaj na okoliš mogao bi se ostvariti razvojem posebnih rješenja za kibersigurnost za sektore koji bi mogli imati veliki utjecaj na okoliš (npr. nuklearne elektrane) kojima bi im se pomoglo da izbjegnu potencijalno katastrofalne posljedice kibernapada na takvu vrstu infrastrukture.

Koliki su troškovi opcije kojoj se daje prednost (ako takve opcije nema, navesti troškove glavnih opcija)?

Troškovi opcije kojoj se daje prednost većinom su povezani s troškovima poslovanja Centra i nacionalnih koordinacijskih centara. Troškovi povezani s provedbom različitih programa financiranja (program Digitalna Europa i program Obzor Europa) predmet su zasebnih procjena učinka.

Kako će to utjecati na poduzeća, MSP-ove i mikropoduzeća?

Mogućnost će najviše utjecati na europska trgovačka društva na strani ponude i potražnje za kibersigurnošću, uključujući na MSP-ove i mikropoduzeća koja djeluju u području kibersigurnosti. Iako im se osnivanjem Centra za stručnost i Mreže ne nameću regulatorne obveze, otvorit će im se mogućnosti za smanjenje troškova osmišljavanja novih proizvoda i pomoći će im se da lakše pristupe zajednici ulagača i privuku potrebna sredstva za primjenu utrživih rješenja. Pristup objektima za testiranje i eksperimentiranje koji se financiraju iz državnog proračuna posebno je važan za MSP-ove i mikropoduzeća jer oni nemaju sredstva za kupnju potrebne infrastrukture ili za putovanje izvan svojeg tržišta (često i izvan EU-a) radi pronalaženja takve infrastrukture. Postoji nada i da bi se ovom inicijativom otvorila nova tržišta za europske MSP-ove i mikropoduzeća koji djeluju u području kibersigurnosti. Nadalje, odabranim mehanizmom osigurat će se koordinacija između istraživanja i industrije i stoga će se istraživanje usmjeriti na konkretne potrebe u industriji. Pružanjem najnaprednijeg stručnog znanja i alata u području kibersigurnosti neizravno će se podupirati gospodarski subjekti da se usklade s Direktivom o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije.

Hoće li to znatno utjecati na nacionalne proračune i uprave?

Inicijativom će se državama članicama omogućiti da koordiniraju ulaganja u potrebnu infrastrukturu za kibersigurnost na nacionalnoj i europskoj razini. Mehanizmom će se omogućiti udruživanje sredstava za alate i infrastrukture koji bi inače bili skuplji ili ih pojedinačne države članice ne bi mogle priuštiti. Takvim pristupom omogućilo bi se stvaranje ekonomija razmjera i racionalizacija. Financijski doprinos država članica Centru za stručnost i relevantnim mjerama trebao bi biti razmjeran doprinosu Unije.

Očekuju li se drugi bitni učinci?

Da, inicijativa nedvojbeno ima pozitivan učinak jer će se njome vjerojatno znatno povećati sposobnosti država članica da neovisno zaštite svoja gospodarstva, među ostalim zaštitom ključnih sektora i povećanjem konkurentnosti europskih poduzeća u području kibersigurnosti i industrija u različitim sektorima, koji će moći prikladno zaštititi svoju postojeću imovinu i osmisliti sigurne, inovativne proizvode uz manje troškove istraživanja i razvoja u području sigurnosti. Time bi se u konačnici trebalo EU-u omogućiti da postane predvodnik sljedeće generacije digitalnih tehnologija i tehnologija za kibersigurnost.

D. Daljnje mjere

Kad će se politika preispitati?

U pravni instrument uključit će se izričita odredba o praćenju ključnih pokazatelja uspješnosti (KPI) te odredba o evaluaciji i preispitivanju u skladu s kojima će Komisija provoditi evaluaciju na sredini provedbenog razdoblja kako bi izmjerila učinak instrumenta i njegovu dodanu vrijednost. Europska komisija nakon toga će izvijestiti Europski parlament i Vijeće. Nakon te evaluacije Komisija može predložiti reviziju i proširenje mandata Centra za stručnost i Mreže.