Svet
Evropske unije

Bruselj, 13. september 2018
(OR. en)

12104/18
ADD 5

Medinstitucionalna zadeva:
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

SPREMNI DOPIS

Pošiljatelj:	za generalnega sekretarja Evropske komisije: direktor Jordi AYET PUIGARNAU
Datum prejema:	12. september 2018
Prejemnik:	generalni sekretar Sveta Evropske unije Jeppe TRANHOLM-MIKKELSEN
Št. dok. Kom.:	SWD(2018) 404 final
Zadeva:	DELOVNI DOKUMENT SLUŽB KOMISIJE POVZETEK OCENE UČINKA Spremni dokument k PREDLOGU UREDBE EVROPSKEGA PARLAMENTA IN SVETA o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov

V prilogi vam pošiljamo dokument SWD(2018) 404 final.

Priloga: SWD(2018) 404 final

EVROPSKA
KOMISIJA

Bruselj, 12.9.2018
SWD(2018) 404 final

DELOVNI DOKUMENT SLUŽB KOMISIJE

POVZETEK OCENE UČINKA

Spremni dokument

k PREDLOGU UREDBE EVROPSKEGA PARLAMENTA IN SVETA

o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov

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

Povzetek

Ocena učinka o predlogu za ustanovitev mreže strokovnih centrov ter Evropskega raziskovalnega in strokovnega centra za kibernetsko varnost

A. Nujnost ukrepanja

Zakaj? V čem je težava?

EU danes še vedno nima dovolj tehnoloških in industrijskih zmogljivosti, da bi samostojno zaščitila svoje gospodarstvo in kritično infrastrukturo ter postala vodilna na svetu na področju kibernetske varnosti. Namen zadevne pobude je prispevati k odpravljanju naslednjih vzrokov in povezanih dejavnikov, ki prispevajo k tem razmeram:

Težava 1: nezadostno strateško in trajnostno usklajevanje in sodelovanje med panogami, raziskovalnimi skupnostmi za kibernetsko varnost in vladami za zaščito gospodarstva, družbe in demokracije z vrhunskimi evropskimi rešitvami za kibernetsko varnost.

Težava 2: premajhne naložbe in omejen dostop do strokovnega znanja, veščin in zmogljivosti na področju kibernetske varnosti po vsej Evropi.

Težava 3: le malo evropskih rezultatov raziskav in inovacij na področju kibernetske varnosti je bilo prenesenih v tržne rešitve in obširno uporabljenih v gospodarstvu.

Osnovnih vzrokov za te težave je veliko, vključno z nezadostnim zaupanjem med različnimi akterji na trgu kibernetske varnosti, neizogibnimi omejitvami obstoječih mehanizmov sodelovanja in mehanizmov za združevanje sredstev, neobstojem okvira za skupno javno naročanje drage infrastrukture za kibernetsko varnost in izdelkov/rešitev za kibernetsko varnost ter neizkoriščenim potencialom tržnih mehanizmov odbijanja in privlačevanja, t. i. „push-pull" mehanizmov.

Kaj naj bi prinesla ta pobuda?

Namen pobude je zagotoviti, da EU ohrani in razvije bistvene (tehnološke in industrijske) zmogljivosti za samostojno zaščito svojega gospodarstva, družbe in demokracije, ter da imajo države članice koristi od najnaprednejših rešitev za kibernetsko varnost in zmogljivosti za kibernetsko obrambo. Njen namen je tudi izboljšati svetovno konkurenčnost podjetij EU za kibernetsko varnost ter evropskim panogam v različnih sektorjih zagotoviti dostop do zmogljivosti in virov, ki jim bodo omogočili pretvorbo kibernetske varnosti v konkurenčno prednost. To bi bilo treba doseči z razvojem učinkovitih mehanizmov za dolgoročno strateško sodelovanje vseh zadevnih akterjev (javnih organov, industrijskih panog in raziskovalnih skupnosti s civilnega in obrambnega področja), z združevanjem znanja in virov za zagotovitev vrhunskih zmogljivosti in infrastrukture, s spodbujanjem obsežne uporabe evropskih izdelkov in rešitev za kibernetsko varnost v gospodarstvu in javnem sektorju, s podpiranjem zagonskih podjetij in MSP na področju kibernetske varnosti ter prizadevanji za zapolnitev vrzeli v znanjih in spretnostih na področju kibernetske varnosti.

Kakšna je dodana vrednost ukrepanja na ravni EU?

Pobuda bi s prispevanjem k nastanku medsebojno povezanega vseevropskega industrijskega in raziskovalnega ekosistema na področju kibernetske varnosti prinesla dodano vrednost zdajšnjim prizadevanjem na nacionalni ravni. Spodbudila naj bi boljše sodelovanje med zadevnimi zainteresiranimi stranmi (tudi med civilnim in obrambnim sektorjem na področju kibernetske varnosti), da bi se kar najbolje uporabili obstoječi viri in strokovno znanje z vse Evrope na področju kibernetske varnosti. EU in državam članicam naj bi pomagala zavzeti proaktivno, dolgoročno in strateško stališče v zvezi z industrijsko politiko za kibernetsko varnost, ki se ne bi omejila le na raziskave in razvoj. Ta pristop naj bi prispeval ne le k prebojnim rešitvam za kibernetskovarnostne izzive, s katerimi se soočata zasebni in javni sektor, ampak tudi podpiral učinkovito uvajanje teh rešitev. Ustreznim raziskovalnim in industrijskim skupnostim ter javnim organom bo prav tako omogočilo, da pridobijo dostop do ključnih zmogljivosti, kot so obrati za preskušanje in poskuse, ki državam članicam zaradi nezadostnih finančnih in človeških vriov pogosto niso dostopne. Prav tako bo z zagotavljanjem dostopa najbolj nadarjenih posameznikov do obsežnih evropskih projektov in s tem zanimivih poklicnih izzivov prispevalo k zapolnitvi vrzeli v znanju in spretnostih ter preprečevanju bega možganov. Vse navedeno se šteje za potrebno, da bi Evropa v svetu postala priznana kot vodilna na področju kibernetske varnosti.

B. Rešitve

Katere zakonodajne in nezakonodajne možnosti politike so se upoštevale? Ali ima katera od njih prednost? Zakaj?

Upoštevalo se je več možnosti politike, tako zakonodajne kot tudi nezakonodajne. Naslednje možnosti so se ohranile za poglobljeno oceno:

1. **osnovni scenarij –** možnost sodelovanja – predvideva nadaljevanje sedanjega pristopa k izgradnji industrijskih in tehnoloških zmogljivosti za kibernetsko varnost v EU s pomočjo podpore za raziskave in inovacije ter povezanih mehanizmov za sodelovanje v okviru programa Obzorje Evropa;
2. **možnost 1:** strokovna mreža za kibernetsko varnost z Evropskim industrijskim, tehnološkim in raziskovalnim strokovnim centrom za kibernetsko varnost, pooblaščenim za uresničevanje ukrepov v podporo industrijskim tehnologijam ter na področju raziskav in inovacij;
3. **možnost 2:** strokovna mreža za kibernetsko varnost z Evropskim raziskovalnim in strokovnim centrom za kibernetsko varnost, z omejitvijo delovanja le na področju raziskav in inovacij.

Možnosti, ki so bile zavrnjene že na začetku, so naslednje: (1) brez ukrepanja; (2) le mreža obstoječih strokovnih centrov in (3) uporaba obstoječe agencije (ENISA, REA ali INEA).

Z vidika splošne zaveze, ki jo je Komisija že dala v zvezi s to pobudo, in z vidika pomembne vloge, ki jo bodo imele države članice, je glavna razlika med obema možnostma politike, ki sta bili podrobno analizirani, njun obseg, kot izhaja iz njune pravne podlage: subjekt, ki bi temeljil le na členu 187 PDEU (možnost 2), bi pobudo omejil na področje raziskav in inovacij ter bi običajno predvideval finančni prispevek zasebnih akterjev. Po drugi strani pa bi subjekt, ki bi imel dvojno pravno podlago – člena 187 in 173 PDEU (možnost 1) –, pomenil širši mandat, ki bi med drugim obsegal tudi uporabo in industrijsko podporo ter ustvarjanje močnejših sinergij s kibernetsko obrambo. Poleg tega bi imele države članice tudi vidnejšo vlogo – tako z vidika udeležbe pri upravljanju kot tudi z vidika potencialnih naročnikov tehnologije kibernetske varnosti.

Analiza je pokazala, da je možnost 1 najprimernejša za doseganje ciljev pobude, hkrati pa zagotavlja največji gospodarski in družbeni učinek in vpliv na okolje ter ščiti interese Unije. Glavne trditve v podporo tej možnosti so vključevale prožnost za omogočanje različnih modelov sodelovanja s skupnostjo in mrežo strokovnih centrov za optimizacijo uporabe obstoječega znanja in virov; zmožnost strukturiranja sodelovanja javnih in zasebnih zainteresiranih strani iz vseh ustreznih sektorjev, vključno z obrambnim; zmožnost oblikovanja prave industrijske politike na področju kibernetske varnosti s podporo dejavnostim, ki niso povezane le z raziskavami in razvojem, ampak tudi z uporabo na trgu. Nenazadnje, možnost 1 poleg tega omogoča izboljšanje skladnosti, saj deluje kot mehanizem za izvajanje s kibernetsko varnostjo povezanega financiranja iz programa za digitalno Evropo in programa Obzorje Evropa, ter krepi sinergije med civilno in obrambno razsežnostjo kibernetske varnosti v zvezi z evropskim obrambnim skladom.

Kdo podpira katero možnost?

Glede na izid posvetovanja in postopkov zbiranja dokazov obstaja jasna potreba po tem, da bi imeli industrijska in raziskovalna skupnost mehanizem, ki bi EU omogočal usklajeno industrijsko politiko na področju kibernetske varnosti, ki bi presegala zgolj dejavnosti raziskav in razvoja, če želi Evropa postati vodilna na svetu na področju kibernetske varnosti. Hkrati so zainteresirane strani poudarile, da bo za uspeh ključna dobro opredeljena vloga centra pri podpori in olajšanju prizadevanj mreže in ustreznih skupnosti ter vključujoč, sodelovalen pristop k mreži, da se prepreči nastanek novih ozkih okvirov delovanja. Struktura bi morala prav tako biti prožna, tako da jo je mogoče enostavno prilagoditi, glede na to, da je kibernetska varnost hitro razvijajoče se okolje. Države članice so skozi celoten postopek poudarjale, da je treba vključiti vse države članice in njihove obstoječe centre odličnosti in strokovne centre ter posebno pozornost nameniti dopolnjevanju ukrepov. Zlasti v zvezi s centrom so države članice poudarile pomen njegove usklajevalne vloge v podporo mreži. Zato bo vsaka pobuda Komisije morala najti pravo ravnovesje med strukturami upravljanja in izvajanja ter ga uporabiti tako, da se bo zagotovilo učinkovito evropsko usklajevanje, ob upoštevanju razvojnih dogodkov na nacionalni ravni.

C. Učinki prednostne možnosti

Kakšne so koristi prednostne možnosti (če obstaja, sicer glavnih možnosti)?

Prednostna možnost bo javnim organom in panogam v državah članicah omogočila učinkovitejše preprečevanje kibernetskih groženj in odzivanje nanje, in sicer z zagotavljanjem več varnih izdelkov in rešitev ter njihovo uporabo. To je zlasti pomembno za zaščito dostopa do bistvenih storitev (npr. prevoznih, zdravstvenih, bančnih in finančnih storitev). Poleg tega bi pozitivno vplivala tudi na konkurenčnost EU in MSP, saj predvideva oblikovanje mehanizma, zmožnega oblikovati industrijske zmogljivosti za kibernetsko varnost v državah članicah in EU, ter učinkovito pretvorbo evropske znanstvene odličnosti v tržne rešitve, ki bi jih bilo mogoče uporabiti v gospodarstvu. Ta možnost omogoča združevanje sredstev za naložbe v nujne zmogljivosti na ravni držav članic in razvoj evropskih skupnih sredstev, ob hkratnem doseganju ekonomije obsega. To bo verjetno izboljšalo dostop do takih zmogljivosti za MSP, industrijo in raziskovalce, kar bo spodbudilo inovacije in skrajšalo razvojne procese. Prav tako bo nekaterim podjetjem na strani povpraševanja znižalo stroške in jim pomagalo kibernetsko varnost pretvoriti v konkurenčno prednost. Možnost omogoča izkoriščanje tržnih priložnosti dvojne rabe, tako da obrambni in civilni skupnosti omogoča sodelovanje pri skupnih izzivih. Prav tako bo verjetno prispevalo dodano vrednost k nacionalnim prizadevanjem v zvezi z obravnavo vrzeli v znanjih in spretnostih na področju kibernetske varnosti. Na ravni EU pa ta možnost omogoča tudi izboljšanje skladnosti in sinergij med različnimi mehanizmi financiranja.

Posreden pozitivni učinek na okolje bi bilo mogoče doseči z razvojem specifičnih rešitev na področju kibernetske varnosti za sektorje, ki lahko imajo velik vpliv na okolje (npr. jedrske elektrarne), ki bi pripomogle k preprečevanju potencialno uničujočih posledic kibernetskih napadov na tovrstno infrastrukturo.

Kakšni so stroški prednostne možnosti (če obstaja, sicer glavnih možnosti)?

Stroški, povezani s prednostno možnostjo, so zlasti povezani s stroški delovanja centra in nacionalnih koordinacijskih centrov. Stroški, povezani z izvajanjem različnih programov financiranja (programa za digitalno Evropo in programa Obzorje Evropa), so ocenjeni v ločenih ocenah učinka.

Kakšen bo vpliv na podjetja, MSP ter mikropodjetja?

Evropska podjetja na področju kibernetske varnosti, tako na strani povpraševanja kot tudi na strani ponudbe, vključno z MSP in mikro podjetji, ki delujejo na področju kibernetske varnosti, bodo skupine zainteresiranih strani, ki bodo občutile največji vpliv. Z ustanovitvijo strokovnega centra in mreže jim sicer ne bodo naložene nobene regulativne obveznosti, bodo pa zaradi ustanovitve imela možnosti za znižanje stroškov zasnove novih izdelkov, lažje bodo dostopala do skupnosti vlagateljev in privabljala financiranje, potrebno za uporabo tržnih rešitev. Za MSP in mikropodjetja je dostop do javno financiranih obratov za preskušanje in poskuse celo pomembnejši, saj jim primanjkuje sredstev za nakup potrebne infrastrukture ali za pot zunaj njihovega trga (in pogosto tudi zunaj EU), da bi našla potrebno infrastrukturo. Obstaja tudi upanje, da bo ta pobuda evropskim MSP in mikro podjetjem, dejavnim na področju kibernetske varnosti, odprla nove trge. Poleg tega bo izbrani mehanizem zagotovil usklajevanje med raziskovanjem in industrijo ter tako raziskovalna prizadevanja usmeril v konkretne potrebe industrije. Zagotovljeno vrhunsko strokovno znanje in orodja na področju kibernetske varnosti bodo posredno podpirali gospodarske subjekte pri izpolnjevanju določb direktive o varnosti omrežij in informacijskih sistemov.

Ali bo prišlo do znatnih učinkov na nacionalne proračune in uprave?

Pobuda bo državam članicam omogočila usklajevanje naložb v potrebno infrastrukturo za kibernetsko varnost na nacionalni in evropski ravni. Mehanizem bo omogočal združevanje virov za orodja in infrastrukturo, ki bi bili v nasprotnem primeru dražji ali si jih države članice posamezno ne bi mogle privoščiti. Tak pristop bi omogočil ekonomijo obsega in racionalizacijo. Finančni prispevek držav članic za strokovni center in ustrezne ukrepe bi moral biti sorazmeren s prispevkom Unije.

Bo imela pobuda druge pomembnejše učinke?

Da. Pobuda ima jasen pozitiven učinek, saj bo po vsej verjetnosti precej povečala zmogljivosti držav članic za samostojno zaščito njihovih gospodarstev, vključno z zaščito kritičnih sektorjev ter povečanjem konkurenčnosti evropskih podjetij, ki se ukvarjajo s kibernetsko varnostjo, in industrijskih panog v različnih sektorjih, saj bodo ta lahko ustrezno zaščitila svoja obstoječa sredstva in zasnovala varne inovativne izdelke, hkrati pa znižala stroške z varnostjo povezanih raziskav in razvoja. Tako bi morala EU na koncu postati vodilna na področju digitalnih tehnologij in tehnologij kibernetske varnosti naslednje generacije.

D. Spremljanje izvajanja

Kdaj se bo politika pregledala?

V pravni instrument bo vključena izrecna klavzula o spremljanju ključnih kazalnikov uspešnosti in tudi klavzula o oceni in pregledu, v skladu s katero bo Evropska komisija izvedla vmesno oceno za merjenje učinka instrumenta in njegove dodane vrednosti. Evropska komisija bo nato poročala Evropskemu parlamentu in Svetu. Po tej oceni lahko Komisija predlaga pregled in podaljšanje mandata strokovnega centra in mreže.