Consiliul
Uniunii Europene

Bruxelles, 13 septembrie 2018
(OR. en)

12104/18
ADD 5

Dosar interinstituțional:
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

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretar general al Comisiei Europene, sub semnătura dlui Jordi AYET PUIGARNAU, director
Data primirii:	12 septembrie 2018
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	SWD(2018) 404 final
Subiect:	DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI REZUMATUL EVALUĂRII IMPACTULUI care însoţeşte documentul PROPUNERE DE REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI de instituire a Centrului european de competențe industriale, tehnologice și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare

În anexă, se pune la dispoziția delegațiilor documentul SWD(2018) 404 final.

Anexă: SWD(2018) 404 final

COMISIA
EUROPEANĂ

Bruxelles, 12.9.2018
SWD(2018) 404 final

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMATUL EVALUĂRII IMPACTULUI

care însoţeşte documentul

PROPUNERE DE REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

de instituire a Centrului european de competențe industriale, tehnologice și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare

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

Fișă rezumat

Evaluarea impactului privind: Propunerea de instituire a Rețelei de centre de competențe și a Centrului european de competențe și de cercetare în domeniul securității cibernetice

A. Necesitatea de a acționa

De ce? Care este problema abordată?

În prezent, UE nu dispune încă de suficiente capacități tehnologice și industriale pentru a-și proteja în mod autonom economia și infrastructurile critice și pentru a deveni un lider global în domeniul securității cibernetice. Prezenta inițiativă urmărește să contribuie la abordarea următoarelor probleme și a factorilor responsabili de această situație:

Problema 1: Nivelul insuficient de coordonare și cooperare strategică și durabilă între sectoarele economice, comunitățile de cercetare în domeniul securității cibernetice și guverne pentru a proteja economia, societatea și democrația cu soluții europene de securitate cibernetică de ultimă generaţie;

Problema 2: Investițiile la o scară prea redusă și accesul limitat la know-how-ul, competențele și infrastructurile în materie de securitate cibernetică din întreaga Europă;

Problema 3: Puține rezultate ale cercetării și inovării europene în materie de securitate cibernetică au fost transpuse în soluții care pot fi comercializate și au fost utilizate pe scară largă în întreaga economie.

Aceste probleme au o serie de factori determinanți, inclusiv nivelul insuficient de încredere între diferiții actori de pe piața securității cibernetice, limitările inerente ale mecanismelor de cooperare existente și de punere în comun a fondurilor, lipsa unui cadru pentru achizițiile comune pentru infrastructura costisitoare de securitate cibernetică și produse/soluții de securitate cibernetică, precum și potențialul neutilizat al mecanismelor de stimulare și de atracție ale pieței.

Ce se așteaptă de la această inițiativă?

Inițiativa urmărește să asigure că UE își menține și dezvoltă capacitățile (tehnologice și industriale) esențiale pentru a-și proteja în mod autonom economia digitală, societatea și democrația și că statele membre beneficiază de cele mai avansate soluții de securitate cibernetică și capabilități de apărare cibernetică. De asemenea, inițiativa urmărește sporirea competitivității globale a întreprinderilor UE din sectorul securității cibernetice și garantarea faptului că industriile europene din diferite sectoare au acces la capacități și resurse pentru a transforma securitatea cibernetică în avantajul lor competitiv. Acest lucru ar trebui realizat prin dezvoltarea unor mecanisme eficace de cooperare strategică pe termen lung a tuturor actorilor relevanți (autorități publice, sectoare industriale, comunitatea de cercetare atât din sectorul civil, cât și din domeniul apărării), prin punerea în comun a cunoștințelor și resurselor pentru a furniza capacități și infrastructuri de ultimă generație, prin stimularea unei utilizări la scară largă a produselor și soluțiilor europene de securitate cibernetică din întreaga economie și din sectorul public, prin sprijinirea întreprinderilor nou-înființate și a IMM-urilor din domeniul securității cibernetice, precum și prin eliminarea lacunelor în materie de competențe în domeniul securității cibernetice.

Care este valoarea adăugată a acțiunii la nivelul UE?

Inițiativa ar aduce o valoare adăugată eforturilor actuale de la nivel național prin sprijinirea creării unui ecosistem industrial și de cercetare în materie de securitate cibernetică interconectat la nivel european. Aceasta ar trebui să încurajeze îmbunătățirea cooperării între părțile interesate relevante (inclusiv între sectoarele civil și de apărare ale securității cibernetice) pentru a asigura o utilizare optimă a resurselor și a expertizei existente în materie de securitate cibernetică răspândite în întreaga Europă. Inițiativa ar trebui să ajute UE și statele membre să adopte o perspectivă proactivă și strategică pe termen mai lung față de politica industrială în domeniul securității cibernetice, care trece dincolo de cercetare și inovare. Această abordare ar trebui să contribuie nu doar la găsirea de soluții revoluționare la provocările din domeniul securității cibernetice cu care se confruntă sectoarele privat și public, ci, de asemenea, ar trebui să sprijine implementarea eficientă a acestor soluții. De asemenea, aceasta va permite comunităților relevante de cercetare și industriale, precum și autorităților publice să obțină acces la capacități esențiale, cum ar fi infrastructurile de testare și experimentare, care, în multe cazuri, nu sunt accesibile unui stat membru în mod individual din cauza insuficienței resurselor financiare și umane. De asemenea, inițiativa va contribui la eliminarea lacunelor în materie de competențe și la evitarea exodului creierelor prin asigurarea

accesului celor mai bune talente la proiecte europene pe scară largă, oferindu-le astfel provocări profesionale interesante. Toate elementele de mai sus sunt considerate, de asemenea, necesare pentru ca Europa să fie recunoscută la nivel mondial ca lider în materie de securitate cibernetică.

B. Soluții

Ce opțiuni de politică legislative și nelegislative au fost luate în considerare? Există sau nu o opțiune preferată? De ce?

Au fost luate în considerare o serie de opțiuni de politică, atât legislative, cât și nelegislative. Următoarele opțiuni au fost reținute pentru o analiză aprofundată:

1. **Scenariul de referință** – Opțiunea colaborativă – presupune continuarea abordării actuale de construire a capacităților industriale și tehnologice în materie de securitate cibernetică în UE prin sprijinirea cercetării și inovării și a mecanismelor de colaborare aferente din cadrul programului Orizont Europa;
2. **Opțiunea 1:** O rețea de competențe în materie de securitate cibernetică cu un Centru european de competențe industriale, tehnologice și de cercetare în materie de securitate cibernetică, entitate împuternicită să aplice măsuri în sprijinul tehnologiilor industriale, precum și în domeniul cercetării și inovării;
3. **Opțiunea 2:** O rețea de competențe în materie de securitate cibernetică, cu un Centru european de competențe și de cercetare în domeniul securității cibernetice limitat doar la activități de cercetare și de inovare;

Opțiunile eliminate într-o etapă inițială au inclus 1) lipsa oricărei măsuri; 2) instituirea unei rețele alcătuite doar din centre de competențe existente și 3) utilizarea unei agenții existente (ENISA, REA sau INEA).

Având în vedere angajamentul general asumat deja de Comisie pentru prezenta inițiativă și dat fiind rolul important pe care îl au statele membre, principala distincție dintre cele două opțiuni de politică analizate în detaliu constă în domeniul lor de aplicare, astfel cum se reflectă în temeiul juridic al acestora: o entitate bazată doar pe articolul 187 din TFUE (opțiunea 2) ar limita inițiativa la domeniul cercetării și inovării și ar presupune de regulă o contribuție financiară din partea actorilor privați. Dimpotrivă, o entitate care se bazează pe un temei juridic dublu – articolul 187 din TFUE și articolul 173 din TFUE (opțiunea 1) – ar însemna un mandat mai extins care cuprinde, printre altele, implementarea și sprijinul industrial și crearea unor sinergii mai puternice cu apărarea cibernetică. De asemenea, aceasta le-ar oferi statelor membre un rol mai important – în ceea ce privește atât rolul acestora în guvernanță, cât și rolul acestora ca potențiali achizitori de tehnologie de securitate cibernetică.

Analiza a arătat că opțiunea 1 este cea mai adecvată pentru atingerea obiectivelor inițiativei, oferind în același timp cele mai mari beneficii economice, societale și de mediu și protejând interesele Uniunii. Principalele argumente în favoarea acestei opțiuni au inclus flexibilitatea de a permite ca diferite modele de cooperare cu comunitatea și rețeaua de centre de competențe să optimizeze utilizarea cunoștințelor și resurselor existente; capacitatea de a structura cooperarea între părțile interesate din sectorul public și privat din toate sectoarele relevante, inclusiv apărarea; capacitatea de a crea o adevărată politică industrială în domeniul securității cibernetice, prin sprijinirea unor activități legate nu numai de cercetare și dezvoltare, ci și de introducere pe piață. Nu în ultimul rând, opțiunea 1 permite, de asemenea, o mai mare coerență, acționând ca mecanism de punere în aplicare pentru finanțarea legată de securitatea cibernetică din programele Europa digitală și Orizont Europa și consolidând sinergiile dintre dimensiunea civilă și cea de apărare ale securității cibernetice în ceea ce privește Fondul european de apărare.

Care sunt susținătorii fiecărei opțiuni?

În conformitate cu rezultatul proceselor de consultare și de strângere de probe, există o cerere clară ca atât comunitățile industriale, cât și cele de cercetare să dispună de un mecanism care ar permite UE să aibă o politică industrială coerentă în domeniul securității cibernetice dincolo de activitățile de cercetare și dezvoltare dacă se dorește ca Europa să devină un lider mondial în domeniul securității cibernetice. În același timp, astfel cum au subliniat părțile interesate, cheia succesului va fi un rol bine definit al centrului în sprijinirea și facilitarea eforturilor rețelei și ale comunităților relevante, precum și o abordare bazată pe colaborare, favorabilă incluziunii, față de rețea pentru a evita crearea de noi compartimentări. Structura ar trebui, de asemenea, să fie flexibilă, astfel încât să fie ușor de adaptat, dat fiind că securitatea cibernetică este un mediu cu o evoluție rapidă. Pe parcursul întregului proces, statele membre au evidențiat necesitatea de a fi deschise către participarea tuturor statelor

membre și a centrelor de excelență și de competențe existente ale acestora și de a acorda o atenție deosebită complementarității acțiunilor. În special în ceea ce privește centrul, statele membre au subliniat importanța rolului său de coordonare în sprijinul rețelei. Prin urmare, orice inițiativă a Comisiei va trebui să găsească echilibrul potrivit în ceea ce privește structurile de guvernanță și de punere în aplicare și să reflecte acest echilibru în structurile de guvernanță și de punere în aplicare pentru a asigura o coordonare eficace la nivel european, luând în considerare evoluția situației la nivel național.

C. Impactul opțiunii preferate

Care sunt beneficiile opțiunii preferate (sau ale opțiunilor principale, dacă nu există o opțiune preferată)?

Opțiunea preferată va permite autorităților publice și industriilor din statele membre să prevină într-un mod mai eficace amenințările cibernetice și să răspundă mai eficient la acestea oferind și dotându-se cu produse și soluții mai sigure. Acest lucru este relevant în special pentru protecția accesului la servicii de bază (de exemplu, servicii de transport, servicii de sănătate, servicii bancare și servicii financiare). Aceasta ar avea, de asemenea, un impact pozitiv asupra competitivității UE și a IMM-urilor deoarece presupune crearea unui mecanism capabil de a construi capacitățile industriale în domeniul securității cibernetice ale statelor membre și ale Uniunii și transpunerea eficace a excelenței științifice europene în soluții care pot fi comercializate și care ar putea fi aplicate în întreaga economie. Această opțiune permite punerea în comun a resurselor pentru a investi în capacitățile necesare la nivelul statelor membre și pentru a dezvolta resurse europene comune, permițând în același timp realizarea de economii de scară. Aceasta va determina probabil un acces sporit pentru IMM-uri, industrii și cercetători la astfel de infrastructuri, ceea ce va stimula inovarea și va scurta procesele de dezvoltare. De asemenea, acest lucru va reduce costurile pentru unele întreprinderi din sectoarele cererii și le va sprijini să transforme securitatea cibernetică în avantajul lor competitiv. Opțiunea preferată permite valorificarea oportunităților de pe piața produselor cu dublă utilizare, permițând comunității civile și celei din domeniul apărării să lucreze împreună pentru a face față provocărilor comune. Totodată, aceasta ar putea aduce valoare adăugată eforturilor naționale legate de abordarea deficitului de competențe în materie de securitate cibernetică. La nivelul UE, această opțiune permite, de asemenea, îmbunătățirea coerenței și a sinergiilor dintre diferitele mecanisme de finanțare.

Un impact pozitiv indirect asupra mediului ar putea fi realizat prin dezvoltarea de soluții de securitate cibernetică specifice pentru sectoarele care au în mod potențial un impact imens asupra mediului (de exemplu, centralele nucleare) ajutându-le să evite posibile consecințe devastatoare cauzate de atacuri cibernetice asupra acestui tip de infrastructură.

Care sunt costurile opțiunii preferate (sau ale opțiunilor principale, dacă nu există o opțiune preferată)?

Costurile aferente opțiunii preferate sunt legate, în principal, de costurile aferente funcționării centrului și a centrelor naționale de coordonare. Costurile legate de punerea în aplicare a diferitelor programe de finanțare (Programul Europa digitală și Programul Orizont Europa) fac obiectul unor evaluări ale impactului separate.

Care va fi impactul asupra societăților, IMM-urilor și microîntreprinderilor?

Întreprinderile europene atât din sectoarele cererii, cât și din sectoarele furnizoare din domeniul securității cibernetice, inclusiv IMM-urile și microîntreprinderile care își desfășoară activitatea în domeniul securității cibernetice, vor fi printre grupurile de părți interesate asupra cărora se va înregistra cel mai mare impact. Deși crearea centrului de competențe și a rețelei nu impune obligații de reglementare asupra lor, aceasta va oferi oportunități în ceea ce privește reducerea costurilor pentru proiectarea de noi produse și va sprijini întreprinderile să obțină mai ușor acces la comunitatea investitorilor și să atragă finanțarea necesară pentru a aplica soluții care pot fi comercializate. În cazul IMM-urilor și al microîntreprinderilor, accesul la infrastructuri de testare și experimentare finanțate din fonduri publice este cu atât mai important cu cât acestea nu dispun de resurse pentru a achiziționa sau pentru a intra pe alte piețe (și adesea în afara UE) pentru a găsi infrastructura necesară. Se speră, de asemenea, că această inițiativă ar deschide noi piețe pentru IMM-urile și microîntreprinderile europene care își desfășoară activitatea în domeniul securității cibernetice. În plus, mecanismul ales va asigura coordonarea între cercetare și industrie și, prin urmare, va direcționa eforturile de cercetare spre nevoile industriale concrete. Furnizarea de expertiză și instrumente de ultimă oră în domeniul securității cibernetice va ajuta indirect operatorii economici să se conformeze Directivei privind securitatea cibernetică.

Va exista un impact semnificativ asupra bugetelor și asupra administrațiilor naționale?

Inițiativa va permite statelor membre să își coordoneze investițiile în infrastructura de securitate cibernetică necesară la nivel național și european. Mecanismul va permite punerea în comun a resurselor pentru instrumente și infrastructuri care altfel ar fi mai costisitoare sau inaccesibile pentru state membre individuale. O astfel de abordare ar permite economii de scară și raționalizare. Contribuția financiară din partea statelor membre la centrul de competențe și la măsurile relevante trebuie să fie proporțională cu contribuția Uniunii.

Vor exista și alte impacturi semnificative?

Da, inițiativa are în mod evident un impact pozitiv, întrucât este probabil ca aceasta să crească substanțial capacitățile statelor membre de a-și proteja economiile în mod autonom, inclusiv protejarea sectoarelor critice, creșterea competitivității întreprinderilor europene din domeniul securității cibernetice, precum și a industriilor din diferite sectoare, care vor putea să își protejeze în mod corespunzător activele existente și să creeze produse inovatoare sigure, reducând în același timp costurile cu cercetarea și dezvoltarea legate de securitate. Aceasta ar trebui în cele din urmă să permită UE să devină lider în domeniul tehnologiilor digitale și de securitate cibernetică de generație următoare.

D. Măsuri ulterioare

Când va fi revizuită politica?

O clauză explicită privind monitorizarea indicatorilor-cheie de performanță (*Key Performance Indicators* – KPI), precum și o clauză de evaluare și reexaminare, prin care Comisia Europeană va efectua o evaluare intermediară pentru a măsura impactul instrumentului și valoarea sa adăugată, vor fi incluse în instrumentul juridic. Comisia Europeană va prezenta ulterior un raport Parlamentului European și Consiliului. În urma acestei evaluări, Comisia ar putea propune o revizuire și o extindere a mandatului Centrului de competențe și al rețelei.