Consiliul
Uniunii Europene

Bruxelles, 14 septembrie 2018
(OR. en)

12104/18

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:	COM(2018) 630 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI de instituire a Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare Contribuția Comisiei Europene la reuniunea liderilor din 19-20 septembrie 2018 de la Salzburg

În anexă, se pune la dispoziția delegațiilor documentul COM(2018) 630 final.

Anexă: COM(2018) 630 final

COMISIA
EUROPEANĂ

Bruxelles, 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

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

Contribuția Comisiei Europene la reuniunea liderilor din 19-20 septembrie 2018 de la Salzburg

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Motivele și obiectivele propunerii

Pe măsură ce viața de zi cu zi și economiile devin tot mai dependente de tehnologiile digitale, cetățenii devin din ce în ce mai expuși la incidente cibernetice grave. Viitorul securității depinde de consolidarea capacității de a proteja Uniunea împotriva amenințărilor cibernetice, întrucât atât infrastructura civilă, cât și capacitățile militare se bazează pe sisteme digitale sigure.

Pentru a face față provocărilor din ce în ce mai mari, Uniunea și-a intensificat în mod constant activitățile în acest domeniu, pe baza Strategiei de securitate cibernetică din 2013[1] și a obiectivelor și principiilor sale, pentru a promova un ecosistem cibernetic fiabil, sigur și deschis. În 2016, Uniunea a adoptat primele sale măsuri în domeniul securității cibernetice prin Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului[2] privind securitatea rețelelor și a sistemelor informatice.

Având în vedere evoluția rapidă a domeniului securității cibernetice, în septembrie 2017 Comisia și Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate au prezentat o comunicare comună[3] intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”, cu scopul de a consolida și mai mult reziliența, prevenirea și răspunsul Uniunii la atacurile cibernetice. Comunicarea comună, bazându-se, de asemenea, pe inițiativele anterioare, a prezentat un set de acțiuni propuse, printre care se numără consolidarea Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), crearea unui cadru de certificare voluntară de securitate cibernetică la nivelul Uniunii pentru a spori securitatea cibernetică a produselor și serviciilor în lumea digitală, precum și un plan de acțiune pentru a răspunde rapid și coordonat la incidentele și crizele de securitate cibernetică de mare amploare.

În comunicarea comună s-a recunoscut faptul că este și în interesul strategic al Uniunii să asigure păstrarea și dezvoltarea capacităților tehnologice esențiale în materie de securitate cibernetică, pentru a-și securiza piața unică digitală și, în special, pentru a proteja rețelele și sistemele informatice critice și pentru a furniza servicii de securitate cibernetică esențiale. Uniunea trebuie să fie în măsură să își securizeze în mod autonom activele digitale și să concureze pe piața mondială a securității cibernetice.

În prezent, Uniunea este un importator net de produse și soluții de securitate cibernetică și depinde în mare măsură de furnizori din afara Europei[4]. Piața securității cibernetice este, la nivel mondial, o piață de 600 de miliarde EUR și se preconizează că va crește în următorii cinci ani în medie cu aproximativ 17 % în ceea ce privește cifra vânzărilor, numărul

---

1 COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU: Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat, JOIN(2013) 1 final.

2 Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

3 COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE, JOIN(2017) 450 final.

4 Proiect de raport final al studiului privind piața securității cibernetice, 2018.

întreprinderilor și ocuparea forței de muncă. Cu toate acestea, în clasamentul primelor 20 de țări care, din perspectiva pieței, au rezultate notabile în materie de securitate cibernetică sunt doar 6 state membre[5].

În același timp, în Uniune există o multitudine de cunoștințe de specialitate și de experiență în materie de securitate cibernetică - peste 660 de organizații din întreaga UE au fost înregistrate în inventarierea recentă a centrelor de expertiză în materie de securitate cibernetică, realizată de Comisie[6]. Această expertiză, dacă este transformată în produse și soluții comercializabile, ar putea permite Uniunii să acopere întregul lanț valoric al securității cibernetice. Totuși,eforturile comunităților din cercetare și industrie sunt fragmentate, nu există o aliniere între acestea și o misiune comună, fapt care reduce competitivitatea UE în acest domeniu, precum și capacitatea sa de a-și securiza activele digitale. În prezent, sectoarele relevante pentru securitatea cibernetică (de exemplu, energia, sectorul spațial, transporturile în domeniul apărării) și subdomeniile acestora sunt insuficient sprijinite.[7] Sinergiile dintre sectoarele civile și de apărare relevante pentru securitatea cibernetică nu sunt exploatate pe deplin nici în Europa.

Crearea, în 2016, a parteneriatului public-privat privind securitatea cibernetică în Uniune a reprezentat un prim pas important prin care comunitățile din cercetare, industrie și din sectorul public își unesc eforturile și resursele pentru a facilita cercetarea și inovarea în materie de securitate cibernetică și, în limitele cadrului financiar 2014-2020, acesta ar trebui să conducă la rezultate bune și mai specifice în domeniul cercetării și inovării. Parteneriatul public-privat a permis partenerilor industriali să-și exprime angajamentul cu privire la cheltuielile lor individuale în domeniile stabilite în agenda strategică de cercetare și inovare a parteneriatului.

Cu toate acestea, Uniunea poate realiza investiții la o scară mult mai mare și are nevoie de un mecanism mai eficace care i-ar permite să construiască capacități durabile, să pună în comun eforturi și competențe și să stimuleze dezvoltarea unor soluții inovatoare care să răspundă provocărilor industriale în materie de securitate cibernetică în domeniul noilor tehnologii multiple (de exemplu, inteligența artificială, informatica cuantică, tehnologia *blockchain* și identitățile digitale sigure), precum și în sectoarele critice (de exemplu, transporturi, energie, sănătate, finanțe, guvernare, telecomunicații, producție, apărare, sectorul spațial).

Comunicarea comună a luat în considerare posibilitatea consolidării capacității Uniunii în materie de securitate cibernetică prin intermediul unei rețele de centre de competențe având drept coordonator un centru european de competențe în materie de securitate cibernetică. Aceasta ar urmări să completeze eforturile existente de consolidare a capacităților în acest domeniu la nivelul Uniunii și la nivel național. În comunicarea comună s-a făcut cunoscută intenția Comisiei de a lansa, în 2018, o evaluare a impactului pentru a examina opțiunile disponibile în vederea instituirii acestei structuri. Ca un prim pas și pentru a colecta informații utile pentru abordările viitoare, Comisia a lansat, în cadrul programului Orizont 2020, o fază-pilot care să ajute la reunirea centrelor naționale într-o rețea care să impulsioneze dezvoltarea competențelor și dezvoltarea tehnologică în materie de securitate cibernetică.

În cadrul summitului digital de la Tallinn din septembrie 2017, șefii de stat și de guvern au cerut Uniunii să devină „un lider mondial în domeniul securității cibernetice până în 2025,

---

5 Proiect de raport final al studiului privind piața securității cibernetice, 2018.

6 Rapoarte tehnice ale JRC: Centre europene de expertiză în materie de securitate cibernetică, 2018.

7 Raport tehnic al JRC: Rezultatele exercițiului de inventariere (a se vedea anexele 4 și 5 pentru detalii).

pentru a asigura încrederea și protecția cetățenilor, a consumatorilor și a întreprinderilor online și pentru a permite un internet liber și reglementat juridic."

Concluziile Consiliului[8] adoptate în noiembrie 2017 au invitat Comisia să prezinte rapid o evaluare a impactului cu privire la opțiunile posibile și să propună, până la jumătatea anului 2018, instrumentul juridic relevant pentru punerea în aplicare a inițiativei.

Programul Europa digitală propus de Comisie în luna iunie 2018[9] urmărește să extindă și să maximizeze beneficiile transformării digitale pentru cetățenii și întreprinderile europene în toate domeniile relevante ale politicilor UE, consolidând politicile și sprijinind obiectivele ambițioase ale pieței unice digitale. Programul propune o abordare coerentă și globală în vederea asigurării unei utilizări optime a tehnologiilor avansate și a combinației adecvate de capacitate tehnică și competență umană pentru transformarea digitală – nu numai în domeniul securității cibernetice, ci și în ceea ce privește infrastructura de date inteligente, inteligența artificială, competențele și aplicațiile avansate în industrie și în domeniile de interes public. Aceste elemente sunt interdependente, se susțin reciproc și, atunci când sunt încurajate simultan, pot atinge nivelul necesar pentru a permite succesul economiei datelor.[10] *Programul Orizont Europa* [11] – următorul program-cadru pentru cercetare și inovare al UE, include, de asemenea, securitatea cibernetică în rândul priorităților sale.

În acest context, prezentul regulament propune înființarea unui Centru de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și a unei rețele a centrelor naționale de coordonare. Acest model de cooperare creat special în acest scop ar trebui să funcționeze după cum urmează pentru a stimula ecosistemul european tehnologic și industrial de securitate cibernetică: Centrul de competențe va facilita și va sprijini coordonarea activității rețelei și va contribui la Comunitatea de competențe în materie de securitate cibernetică, direcționând agenda tehnologică în materie de securitate cibernetică și facilitând accesul la expertiza astfel dobândită. Centrul de competențe va realiza acest lucru în special prin implementarea părților relevante ale programelor Europa digitală și Orizont Europa, prin alocarea de granturi și prin efectuarea de achiziții. Având în vedere investițiile considerabile în securitatea cibernetică realizate în alte părți ale lumii și necesitatea coordonării și reunirii resurselor relevante din Europa, Centrul de competențe este propus sub forma unui parteneriat european[12], facilitându-se astfel realizarea de investiții comune de către Uniune, statele membre și/sau industrie. Prin urmare, propunerea prevede că statele membre trebuie să contribuie cu o sumă proporțională la acțiunile Centrului de competențe și ale rețelei. Organismul decizional principal este consiliul de conducere, din care fac parte și statele membre, dar au drept de vot numai acele state care participă financiar. Mecanismul de vot în cadrul consiliului de conducere urmează principiul dublei majorități care presupune

---

8 Concluziile Consiliului privind Comunicarea comună către Parlamentul European și Consiliu - Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE, adoptate de Consiliul Afaceri Generale la 20 noiembrie 2017.

9 COM(2018) 434 Propunere de regulament al Parlamentului European și al Consiliului de instituire a programului Europa digitală pentru perioada 2021-2027.

10 A se vedea SWD(2018) 305.

11 COM (2018) 435 Propunere de regulament al Parlamentului European și al Consiliului de instituire a programului-cadru pentru cercetare și inovare Orizont Europa și de stabilire a normelor sale de participare și de diseminare.

12 Astfel cum se stabilește în COM (2018) 435 Propunere de regulament al Parlamentului European și al Consiliului de instituire a programului-cadru pentru cercetare și inovare Orizont Europa și de stabilire a normelor sale de participare și de diseminare și astfel cum se precizează în COM(2018) 434 Propunere de regulament al Parlamentului European și al Consiliului de instituire a programului Europa digitală pentru perioada 2021-2027.

75 % din contribuția financiară și 75 % din voturi. Având în vederea responsabilitatea care îi revine în ceea ce privește bugetul Uniunii, Comisia deține 50 % din voturi. În activitatea sa privind consiliul de conducere, Comisia va apela, atunci când va fi necesar, la expertiza Serviciului European de Acțiune Externă. Consiliul de conducere este asistat de un Consiliu consultativ pe probleme științifice sau industriale, pentru a asigura un dialog regulat cu sectorul privat, cu organizațiile de consumatori și cu alte părți interesate relevante.

Printr-o colaborare strânsă cu Rețeaua centrelor naționale de coordonare și cu comunitatea de competențe în materie de securitate cibernetică (care implică un grup mare și diversificat de actori din domeniul dezvoltării tehnologiei de securitate cibernetică, cum ar fi entitățile de cercetare, industriile furnizoare, sectoarele cererii și sectorul public) instituită prin prezentul regulament, Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică ar fi principalul organism de execuție pentru resursele financiare ale UE dedicate securității cibernetice în cadrul programelor propuse *Europa digitală* și *Orizont Europa* .

O astfel de abordare cuprinzătoare ar permite sprijinirea securității cibernetice de-a lungul întregului lanț valoric, de la cercetare până la sprijinirea implementării și a adoptării pe scară largă a tehnologiilor-cheie. Participarea financiară a statelor membre ar trebui să fie proporțională cu contribuția financiară a UE la această inițiativă și constituie un element indispensabil pentru reușita acesteia.

Având în vedere expertiza sa deosebită și reprezentarea generală și relevantă a părților interesate, Organizația Europeană de Securitate Cibernetică, care este omologul Comisiei în parteneriatul public-privat contractual privind securitatea cibernetică din cadrul programului Orizont 2020, ar trebui să fie invitată să contribuie la activitatea centrului și a rețelei.

În plus, Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică ar trebui să urmărească sporirea sinergiilor dintre dimensiunile civilă și de apărare ale securității cibernetice. Acesta ar trebui să ofere sprijin statelor membre și altor actori relevanți, oferind consiliere, împărtășind expertiză și facilitând colaborarea cu privire la proiecte și acțiuni. La cererea statelor membre, acesta ar putea acționa, de asemenea, ca administrator de proiect, în special în legătură cu Fondul european de apărare. Prezenta inițiativă își propune să contribuie la rezolvarea următoarelor probleme :

- **Cooperarea insuficientă dintre sectoarele cererii și sectoarele furnizoare în materie de securitate cibernetică** Întreprinderile europene se confruntă cu provocarea pe care o reprezintă atât menținerea securității, cât și oferirea de produse și servicii sigure clienților lor. Cu toate acestea, adesea, nu sunt în măsură să asigure în mod corespunzător securitatea produselor, a serviciilor și a activelor lor existente sau să conceapă produse și servicii inovatoare sigure. Principalele active din domeniul securității cibernetice sunt adesea prea costisitoare pentru a fi dezvoltate și create de actori individuali, a căror activitate economică de bază nu este legată de securitatea cibernetică. În același timp, legăturile dintre cererea și oferta de pe piața securității cibernetice nu sunt suficient de bine dezvoltate, ceea ce duce la o aprovizionare insuficientă cu produse și soluții europene adaptate nevoilor diferitelor sectoare, precum și la niveluri insuficiente de încredere în rândul actorilor de pe piață.
- **Lipsa unui mecanism eficient de cooperare între statele membre în vederea consolidării capacităților industriale.** În prezent, nu există, de asemenea, un mecanism eficient de cooperare pentru ca statele membre să conlucreze în vederea construirii capacităților necesare pentru a sprijini inovarea în materie de securitate cibernetică în toate

sectoarele industriale și pentru a pune în practică soluții europene de securitate cibernetică de vârf. Mecanismele de cooperare în domeniul securității cibernetice existente pentru statele membre, prevăzute în Directiva (UE) 2016/1148, nu prevăd acest tip de activități în mandatul lor.

- **Cooperare insuficientă în cadrul comunităților din industrie și cercetare, precum și între acestea.** În pofida capacității teoretice a Europei de a acoperi întregul lanț valoric al securității cibernetice, există sectoare (de exemplu, energie, sectorul spațial, apărare, transporturi) și subdomenii relevante pentru securitatea cibernetică care sunt în prezent insuficient sprijinite de comunitatea de cercetare sau care sunt sprijinite doar de un număr limitat de centre (de exemplu, criptografie post-cuantică și cuantică, încredere și securitate cibernetică în inteligența artificială). Deși, evident, această colaborare există, foarte adesea este vorba despre un tip de acord pe termen scurt de consultanță, care nu permite implicarea în planuri de cercetare pe termen lung în vederea soluționării provocărilor industriale în materie de securitate cibernetică.
- **Cooperare insuficientă între comunitățile de cercetare și inovare civile și de apărare din domeniul securității cibernetice.** Problema nivelului insuficient de cooperare se regăsește și în cadrul comunităților civile și de apărare. Sinergiile existente nu sunt utilizate pe deplin din cauza lipsei unor mecanisme eficiente care să permită acestor comunități să coopereze în mod eficient și să consolideze încrederea, care, chiar mai mult decât în alte domenii, este o condiție prealabilă pentru o cooperare de succes. La acestea se adaugă capacitățile financiare limitate de pe piața securității cibernetice din UE, inclusiv insuficiența fondurilor pentru sprijinirea inovării.
- **Coerența cu dispozițiile existente în domeniul de politică vizat**

Rețeaua de competențe în materie de securitate cibernetică și Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică vor acționa ca un sprijin suplimentar pentru dispozițiile și actorii existenți din domeniul politicii de securitate cibernetică. Mandatul Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică va fi complementar cu eforturile ENISA, însă are o orientare diferită și necesită un set diferit de competențe. În timp ce mandatul ENISA are în vedere un rol de consiliere în ceea ce privește cercetarea și inovarea în materie de securitate cibernetică în UE, mandatul propus se concentrează în primul rând și în cea mai mare măsură asupra altor sarcini esențiale pentru consolidarea rezilienței în materie de securitate cibernetică în UE. În plus, mandatul ENISA nu are în vedere acele tipuri de activități care ar urma să constituie sarcinile principale ale centrului și ale rețelei - stimularea dezvoltării și a implementării tehnologiei în domeniul securității cibernetice și completarea eforturilor de consolidare a capacităților în acest sector la nivelul UE și la nivel național.

Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, împreună cu Rețeaua de competențe în materie de securitate cibernetică va acționa, de asemenea, în vederea sprijinirii cercetării pentru facilitarea și accelerarea proceselor de standardizare și de certificare, în special a celor legate de sistemele de certificare de securitate cibernetică în sensul Legii propuse privind securitatea cibernetică[13][14].

[13] Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind ENISA, „Agenția UE pentru securitate cibernetică”, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor [„Legea privind securitatea cibernetică”, COM(2017) 477 final/3].

Prezenta inițiativă extinde *de facto* parteneriatul public-privat privind securitatea cibernetică, care a fost prima încercare la nivelul UE de a reuni sectorul securității cibernetice, sectorul cererii (cumpărătorii de produse și soluții de securitate cibernetică, inclusiv administrațiile publice și sectoarele critice cum ar fi, de exemplu, transporturile, sănătatea, energia, sectorul financiar) și comunitatea cercetătorilor, pentru a construi platforma dialogului durabil și a crea condiții pentru coinvestiții voluntare. Parteneriatul public-privat privind securitatea cibernetică fost creat în 2016 și a generat investiții în valoare de până la 1,8 miliarde EUR până în 2020. Cu toate acestea, amploarea investițiilor realizate în alte părți ale lumii (de exemplu, SUA au investit în 2017 19 miliarde USD numai în securitatea cibernetică) arată că UE trebuie să depună mai multe eforturi pentru a atinge o masă critică de investiții și pentru a depăși fragmentarea capacităților dispersate pe teritoriul UE.

- **Coerența cu alte politici ale Uniunii**

Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică va acționa ca un organism unic de punere în aplicare a diferitelor programe ale Uniunii care sprijină securitatea cibernetică (programul Europa digitală și Europa Orizont) și va consolida coerența și sinergiile dintre acestea.

Această inițiativă va permite, de asemenea, completarea eforturilor statelor membre, prin asigurarea unor contribuții adecvate pentru factorii de decizie din domeniul educației, în vederea consolidării competențelor în materie de securitate cibernetică (de exemplu, prin dezvoltarea unor programe de învățământ privind securitatea cibernetică în sistemele educaționale civile și militare), cu scopul de a contribui la dezvoltarea în UE a unei forțe de muncă calificate în ceea ce privește securitatea cibernetică - un atu esențial pentru societățile din domeniul securității cibernetice, precum și pentru alte sectoare interesate de securitatea cibernetică. În ceea ce privește educația și formarea în domeniul apărării cibernetice, această inițiativă va fi coerentă cu activitatea desfășurată în prezent de platforma de educație, formare și exerciții în domeniul apărării cibernetice instituită în cadrul Colegiului European de Securitate și Apărare.

Această inițiativă va completa și va sprijini eforturile depuse de centrele de inovare digitală în cadrul programului Europa Digitală. Centrele de inovare digitală sunt organizații non-profit care ajută întreprinderile – în special întreprinderile nou-înființate, IMM-urile și întreprinderile cu capitalizare medie, să devină mai competitive prin îmbunătățirea proceselor lor de afaceri/de producție, precum și a produselor și serviciilor lor, prin inovare inteligentă facilitată de tehnologia digitală. Centrele de inovare digitală oferă servicii de inovare orientate spre întreprinderi, cum ar fi informații despre piață, consiliere în materie de finanțare, acces la echipamente relevante de testare și experimentare, formare și dezvoltarea competențelor, pentru a ajuta noile produse sau servicii să ajungă pe piață cu succes sau pentru a introduce procese de producție mai bune. Unele centre de inovare digitală, care au expertiză specifică în ceea ce privește securitatea cibernetică, ar putea fi implicate în mod direct în Comunitatea de competențe în materie de securitate cibernetică instituită prin prezenta inițiativă. Cu toate acestea, în majoritatea cazurilor, centrele de inovare digitală care nu au un profil specific de

[14] Acest lucru nu aduce atingere mecanismelor de certificare prevăzute de Regulamentul general privind protecția datelor, în cadrul căruia autoritățile de protecție a datelor au un rol de jucat, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE („Regulamentul general privind protecția datelor”).

securitate cibernetică ar facilita accesul membrilor lor la expertiza, cunoștințele și capacitățile în materie de securitate cibernetică disponibile prin cooperarea strânsă cu Rețeaua de centre naționale de coordonare și cu Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică. Centrele de inovare digitală ar sprijini, de asemenea, implementarea unor produse și soluții inovatoare în materie de securitate cibernetică care să corespundă nevoilor societăților și ale altor utilizatori finali pe care acestea îi deservesc. În cele din urmă, dar nu mai puțin important, centrele de inovare digitală specifice unui sector ar putea să își împărtășească cunoștințele despre nevoile reale din sectorul respectiv cu rețeaua și cu centrul pentru a contribui la procesul de reflecție privind agenda în materie de cercetare și inovare care să răspundă cerințelor industriale.

Se va urmări realizarea de sinergii cu comunitățile de cunoaștere și inovare relevante ale Institutului European de Inovare și Tehnologie, în special cu EIT Digital.

2. TEMEIUL JURIDIC, SUBSIDIARITATEA ȘI PROPORȚIONALITATEA

- **Temeiul juridic**

Centrul de competențe ar trebui să fie instituit pe baza unui dublu temei juridic, având în vedere natura și obiectivele sale specifice. Articolul 187 din TFUE, care stabilește structurile necesare pentru execuția eficientă a programelor de cercetare, de dezvoltare tehnologică și demonstrative ale Uniunii, permite Centrului de competențe să creeze sinergii și să pună în comun resurse pentru a investi în capacitățile necesare la nivelul statelor membre și pentru a dezvolta active comune la nivel european (de exemplu, prin achiziția în comun a infrastructurii necesare de testare și experimentare în materie de securitate cibernetică). Primul paragraf al articolului 188 prevede adoptarea unor astfel de măsuri. Cu toate acestea, primul paragraf al articolului 188 ca temei juridic unic nu ar permite ca activitățile să depășească sfera cercetării și a dezvoltării, după cum este necesar pentru îndeplinirea tuturor obiectivelor Centrului de competențe prevăzute în prezentul regulament, sprijinind introducerea pe piață a produselor și a soluțiilor de securitate cibernetică, ajutând industria europeană de securitate cibernetică să devină mai competitivă și să își sporească cota de piață și adăugând valoare eforturilor naționale de abordare a lacunelor în ceea ce privește competențele în materie de securitate cibernetică. Prin urmare, pentru a atinge aceste obiective este necesar să se adauge articolul 173 alineatul (3) ca temei juridic care permite Uniunii să prevadă măsuri de sprijinire a competitivității acestui sector.

- **Justificare pentru propunere în ceea ce privește subsidiaritatea și principiile proporționalității**

Securitatea cibernetică este o problemă de interes comun pentru Uniune, astfel cum au confirmat concluziile Consiliului menționate anterior. Amploarea și caracterul transfrontalier al unor incidente precum *WannaCry* sau *NonPetya* constituie un argument în acest caz. Natura și amploarea provocărilor tehnologice de securitate cibernetică, precum și coordonarea insuficientă a eforturilor în cadrul industriei, al sectorului public și al comunităților din cercetare, precum și între acestea, impun UE să sprijine în continuare eforturile de coordonare, atât pentru a pune în comun o masă critică de resurse, cât și pentru a asigura o mai bună gestionare a cunoștințelor și a activelor. Acest lucru este necesar având în vedere nevoia de resurse legate de anumite capacități de cercetare, dezvoltare și implementare în materie de securitate cibernetică, necesitatea de a oferi acces la know-how interdisciplinar în materie de securitate cibernetică la nivelul diferitelor discipline (adesea doar parțial disponibile la nivel național), natura globală a lanțurilor valorice industriale, precum și activitatea concurenților mondiali activi pe mai multe piețe.

Acest lucru necesită resurse și expertiză la un nivel pe care acțiunea individuală a oricărui stat membru nu îl poate atinge într-o măsură suficientă. De exemplu, o rețea paneuropeană de comunicații cuantice ar putea necesita investiții UE de aproximativ 900 de milioane EUR, în funcție de investițiile realizate de statele membre (care urmează să fie interconectate/completate) și de măsura în care tehnologia va permite reutilizarea infrastructurilor existente. Inițiativa va avea un rol esențial în punerea în comun a finanțării și va permite realizarea acestui tip de investiție în Uniune.

Obiectivele acestei inițiative nu pot fi realizate pe deplin de către statele membre în mod individual. Astfel cum s-a arătat mai sus, acestea pot fi realizate mai bine la nivelul Uniunii prin punerea în comun a eforturilor și prin evitarea suprapunerii lor inutile, contribuind la atingerea masei critice a investițiilor și asigurând o utilizare optimă a finanțării publice. În același timp, în conformitate cu principiul proporționalității, prezentul regulament nu depășește ceea ce este necesar pentru atingerea acestui obiectiv. Prin urmare, acțiunea UE este justificată din rațiuni de subsidiaritate și proporționalitate.

Instrumentul nu prevede noi obligații de reglementare pentru întreprinderi. În același timp, este foarte probabil ca întreprinderile, în special IMM-urile, să își reducă costurile aferente eforturilor lor de elaborare a unor produse inovatoare sigure din punct de vedere cibernetic, întrucât inițiativa permite punerea în comun a resurselor pentru a se investi în capacitățile necesare la nivelul statelor membre sau pentru a se dezvolta active comune la nivel european (de exemplu, prin achiziția în comun a infrastructurii necesare de testare și experimentare în materie de securitate cibernetică). Aceste active ar putea fi utilizate de către industrii și de către IMM-urile din diferite sectoare pentru a garanta că produsele lor sunt sigure din punct de vedere cibernetic și a transforma securitatea cibernetică în avantajul lor competitiv.

- **Alegerea instrumentului**

Instrumentul propus instituie un organism dedicat punerii în aplicare a acțiunilor de securitate cibernetică din cadrul programelor Europa digitală și Orizont Europa. Acesta prevede mandatul, sarcinile și structura de guvernanță. Pentru înființarea unui astfel de organism al Uniunii, este necesară adoptarea unui regulament.

3. CONSULTĂRILE CU PĂRȚILE INTERESATE ȘI EVALUĂRILE IMPACTULUI

Propunerea de creare a unei Rețele de competențe în materie de securitate cibernetică și a unui Centru de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică constituie o inițiativă nouă. Aceasta are rolul de a continua și de a extinde parteneriatul contractual public-privat privind securitatea cibernetică creat în 2016.

- **Consultările cu părțile interesate**

Securitatea cibernetică este o temă vastă și transsectorială. Comisia a utilizat diferite metode de consultare pentru a se asigura că interesul public general al Uniunii – spre deosebire de interesele speciale ale unui număr restrâns de grupuri de părți interesate – este bine reflectat în această inițiativă. Această metodă asigură transparența și responsabilitatea în activitatea Comisiei. Deși nu s-a realizat nicio consultare publică deschisă în mod specific pentru această inițiativă, având în vedere publicul său țintă (comunitățile din industrie și cercetare și statele membre), tematica a fost deja acoperită prin alte câteva consultări publice deschise:

- o consultare publică deschisă generală, desfășurată în 2018 cu privire la tema investițiilor, a cercetării și inovării, a IMM-urilor și a pieței unice;

- o consultare publică online, cu o durată de 12 săptămâni, lansată în 2017 pentru a se afla punctele de vedere ale publicului larg (aproximativ 90 de respondenți) cu privire la evaluarea și revizuirea activității ENISA;
- o consultare publică online, cu o durată de 12 săptămâni, care a fost efectuată în 2016 cu ocazia lansării parteneriatului contractual public-privat privind securitatea cibernetică (aproximativ 240 de respondenți).

De asemenea, Comisia a organizat consultări specifice cu privire la prezenta inițiativă, inclusiv ateliere, reuniuni și solicitări de contribuții specifice (de la ENISA și de la Agenția Europeană de Apărare). Perioada de consultare a durat mai mult de 6 luni, din noiembrie 2017 până în martie 2018. Comisia a realizat, de asemenea, o inventariere a centrelor de expertiză, care a permis colectarea de informații de la 665 de centre de expertiză în materie de securitate cibernetică în ceea ce privește know-how-ul și activitatea lor, domeniile lor de lucru și cooperarea internațională. Sondajul a fost lansat în ianuarie, iar sondajele transmise până la 8 martie 2018 au fost luate în considerare pentru analiza raportului.

Părțile interesate din comunitățile din industrie și cercetare au considerat că Centrul de competențe și rețeaua ar putea adăuga valoare eforturilor actuale depuse la nivel național, contribuind la crearea unui ecosistem european în materie de securitate cibernetică, fapt ce ar permite o mai bună cooperare între comunitățile din cercetare și din industrie. De asemenea, acestea au considerat că este necesar ca UE și statele membre să adopte o perspectivă proactivă, pe termen mai lung și strategică în ceea ce privește politica industrială în materie de securitate cibernetică, depășind sfera cercetării și inovării. Părțile interesate și-au făcut cunoscută nevoia de a obține acces la capacități esențiale, cum ar fi infrastructurile de testare și experimentare, și de a fi mai ambițioase referitor la eliminarea lacunelor în ceea ce privește competențele în materie de securitate cibernetică, de exemplu prin proiecte europene de anvergură care atrag cele mai bune talente. Toate cele de mai sus au fost, de asemenea, considerate necesare pentru ca Uniunea să fie recunoscută la nivel mondial ca lider în domeniul securității cibernetice.

În cadrul activităților de consultare desfășurate începând din luna septembrie a anului trecut[15], precum și în cadrul concluziilor Consiliului dedicate acestui subiect[16], statele membre au salutat intenția de a se institui o rețea de competențe în materie de securitate cibernetică pentru a stimula dezvoltarea și implementarea tehnologiilor de securitate cibernetică, subliniind necesitatea ca aceasta să fie deschisă tuturor statelor membre și centrelor lor existente de excelență și de competențe și de a se acorda o atenție deosebită complementarității. În ceea ce privește în mod specific viitorul Centru de competențe, statele membre au subliniat importanța rolului său de coordonator în sprijinul rețelei. În special referitor la activitățile și nevoile naționale în materie de apărare cibernetică, exercițiul de inventariere a nevoilor statelor membre în materie de apărare cibernetică efectuat de Serviciul European de Acțiune Externă în luna martie 2018 a demonstrat faptul că majoritatea statelor membre consideră că sprijinul UE în domeniul formării și educației în domeniul cibernetic și pentru industrie prin cercetare și dezvoltare constituie o valoare adăugată.[17] Într-adevăr, inițiativa ar fi pusă în aplicare împreună cu statele membre sau cu entitățile sprijinite de

---

15 De exemplu, masa rotundă la nivel înalt cu statele membre, vicepreședintele Ansip și comisarul Gabriel din 5 decembrie 2017

16 Consiliul Afaceri Generale: Concluziile Consiliului privind Comunicarea comună către Parlamentul European și Consiliu - Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE (20 noiembrie 2017)

17 SEAE, martie 2018

acestea. Colaborările dintre comunitățile din industrie, din cercetare și/sau din sectorul public ar reuni și ar consolida entitățile și eforturile existente și nu ar crea unele noi. De asemenea, statele membre ar fi, de asemenea, implicate în definirea unor acțiuni specifice care să vizeze sectorul public, în calitate de utilizator direct al tehnologiei și know-how-ului în materie de securitate cibernetică.

- **Evaluarea impactului**

O evaluare a impactului care sprijină această inițiativă a fost înaintată Comitetului de analiză a reglementării la 11 aprilie 2017 și a primit un aviz pozitiv cu rezerve. Evaluarea impactului a fost revizuită ulterior, avându-se în vedere observațiile comitetului. Avizul comitetului și anexa în care se explică cum s-a ținut seama de observațiile comitetului se publică odată cu propunerea.

În cadrul evaluării impactului au fost luate în considerare o serie de opțiuni de politică, atât legislative, cât și nelegislative. Pentru o evaluare aprofundată au fost reținute următoarele opțiuni:

- Scenariul de referință - Opțiunea de colaborare - presupune continuarea abordării actuale în ceea ce privește consolidarea capacităților industriale și tehnologice de securitate cibernetică în UE prin sprijinirea cercetării și inovării și a mecanismelor conexe de colaborare în cadrul PC9.
- Opțiunea 1: O rețea de competențe în materie de securitate cibernetică, alături de un Centru de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică având mandatul dublu de a adopta măsuri de sprijinire a tehnologiilor industriale, precum și în domeniul cercetării și inovării.
- Opțiunea 2: O rețea de competențe în materie de securitate cibernetică, alături de un Centru european de competențe și de cercetare în materie de securitate cibernetică axat pe activități de cercetare și de inovare

Printre opțiunile eliminate într-o primă fază s-au numărat 1) opțiunea de a nu întreprinde nicio acțiune, 2) opțiunea de a crea doar rețeaua de competențe în materie de securitate cibernetică, 3) opțiunea de a crea doar o structură centralizată, precum și 4) opțiunea de a utiliza o agenție existentă [Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), Agenția Executivă pentru Cercetare (REA) sau Agenția Executivă pentru Inovare și Rețele (INEA)].

În urma analizei s-a ajuns la concluzia că opțiunea 1 este cea mai potrivită pentru a se atinge obiectivele inițiativei, asigurând, în același timp, cel mai mare impact economic, societal și de mediu și protejând interesele Uniunii. Printre principalele argumente în favoarea acestei opțiuni s-au numărat capacitatea de a crea o politică industrială privind securitatea cibernetică reală, prin sprijinirea activităților legate nu doar de cercetare și dezvoltare, ci și de implementarea pe piață, flexibilitatea de a permite diferite modele de cooperare cu rețeaua centrelor de competențe pentru a optimiza utilizarea cunoștințelor și a resurselor existente, capacitatea de a structura cooperarea și angajamentele comune ale părților interesate din sectorul public și privat provenind din toate sectoarele relevante, inclusiv din domeniul apărării. În cele din urmă, dar nu mai puțin important, opțiunea 1 permite, de asemenea, sporirea sinergiilor și poate acționa ca un mecanism de punere în aplicare pentru două fluxuri diferite de finanțare ale UE pentru securitatea cibernetică în contextul următorului cadru financiar multianual (programul Europa digitală și programul Orizont Europa).

- **Drepturile fundamentale**

Prezenta inițiativă va permite autorităților publice și industriilor din statele membre să prevină și să răspundă cu mai multă eficacitate la amenințările cibernetice, oferind și dotându-se cu produse și soluții mai sigure. Acest lucru este în special relevant pentru protecția accesului la servicii esențiale (de exemplu, servicii de transport, de sănătate, bancare și financiare).

De asemenea, o capacitate sporită a Uniunii Europene de a-și securiza în mod autonom produsele și serviciile îi poate ajuta pe cetățeni să se bucure de drepturile și valorile lor democratice (de exemplu, să își protejeze mai bine drepturile legate de informații consacrate în Carta drepturilor fundamentale, în special dreptul la protecția datelor cu caracter personal și la viața privată) și, în consecință, să le sporească încrederea în societatea și economia digitală.

4. IMPLICAȚII BUGETARE

Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, în cooperare cu rețeaua de competențe în materie de securitate cibernetică, va fi principalul organism de execuție a resurselor financiare ale UE dedicate securității cibernetice în cadrul programelor Europa digitală și Orizont Europa.

Implicațiile bugetare legate de punerea în aplicare a programului Europa digitală sunt enumerate în detaliu în Fișa financiară legislativă anexată la prezenta propunere. Contribuția din pachetul financiar al clusterului „O societate sigură și favorabilă incluziunii” din cadrul pilonului II „Provocările globale și competitivitatea industrială” al programului Orizont Europa (pachetul financiar total este de 2 800 000 000 EUR) menționat la articolul 21 alineatul (1) litera (b) va fi propusă de Comisie în cursul procesului legislativ și, în orice caz, înainte de a se ajunge la un acord politic. Propunerea se va baza pe rezultatele procesului de planificare strategică, astfel cum este definit la articolul 6 alineatul (6) din Regulamentul XXX [programul-cadru Orizont Europa].

5. ALTE ELEMENTE

- **Planurile de punere în aplicare și măsurile de monitorizare, evaluare și raportare**

În prezenta propunere (articolul 38) se prevede clauză de evaluare explicită prin care Comisia va efectua o evaluare independentă. Comisia va trimite ulterior Parlamentului European și Consiliului un raport privind evaluarea sa, însoțit, după caz, de o propunere de revizuire, pentru a măsura impactul și valoarea adăugată a instrumentului. Se va aplica metodologia de evaluare prevăzută de măsurile Comisiei privind o mai bună legiferare.

Directorul executiv ar trebui să prezinte consiliului de conducere, la fiecare doi ani, o evaluare ex-post a activităților Centrului de competențe european industrial, tehnologic și de cercetare și ale rețelei, după cum se prevede la articolul 17 din prezenta propunere. De asemenea, directorul executiv ar trebui să elaboreze un plan de măsuri ulterioare în ceea ce privește concluziile evaluărilor retrospective și să prezinte Comisiei, la fiecare doi ani, un raport privind progresele înregistrate. Consiliul de conducere ar trebui să fie responsabil cu monitorizarea acțiunilor adecvate întreprinse ca urmare a acestor concluzii, astfel cum se prevede la articolul 16 din prezenta propunere.

Presupusele cazuri de administrare defectuoasă a activităților organismului juridic pot face obiectul investigațiilor efectuate de Ombudsmanul European în conformitate cu prevederile articolului 228 din tratat.

2018/0328 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

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

Contribuția Comisiei Europene la reuniunea liderilor din 19-20 septembrie 2018 de la Salzburg

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 173 alineatul (3) și articolul 188 primul paragraf,

având în vedere propunerea Comisiei Europene,

având în vedere avizul Comitetului Economic și Social European[18],

având în vedere avizul Comitetului Regiunilor[19],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Viața noastră de zi cu zi și economiile noastre devin din ce în ce mai dependente de tehnologiile digitale, iar cetățenii sunt din ce în ce mai expuși la incidente cibernetice grave. Viitorul securității depinde, printre altele, de consolidarea capacității tehnologice și industriale de a proteja Uniunea împotriva amenințărilor cibernetice, întrucât atât infrastructura civilă, cât și capacitățile militare depind de sisteme digitale sigure.

(2) Uniunea și-a intensificat în mod constant activitățile pentru a răspunde provocărilor din ce în ce mai mari în materie de securitate cibernetică, în urma Strategiei de securitate cibernetică din 2013[20], care vizează promovarea unui ecosistem cibernetic fiabil, sigur și deschis. În 2016, Uniunea a adoptat primele măsuri în domeniul securității cibernetice prin Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului[21] privind securitatea rețelelor și a sistemelor informatice.

---

18 JO C , p. .

19 JO C , , p. .

20 Comunicare comună către Parlamentul European și Consiliu: Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat, JOIN(2013) 1 final.

21 Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

(3) În septembrie 2017, Comisia și Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate au prezentat o comunicare comună[22] intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”, cu scopul de a consolida și mai mult reziliența, capacitatea de descurajare și răspunsul UE la atacurile cibernetice.

(4) În cadrul summitului digital de la Tallinn din septembrie 2017, șefii de stat și de guvern au lansat Uniunii apelul de a ocupa „o poziție de lider mondial în domeniul securității cibernetice până în 2025, pentru a asigura protecția cetățenilor, a consumatorilor și a întreprinderilor noastre online, precum și pentru a câștiga încrederea acestora, dar și pentru a permite un internet liber și aflat sub incidența legii.”

(5) O perturbare semnificativă a rețelelor și a sistemelor informatice poate afecta statele membre și Uniunea în ansamblu. Prin urmare, securitatea rețelelor și a sistemelor informatice este esențială pentru buna funcționare a pieței interne. În prezent, Uniunea depinde de furnizorii de securitate cibernetică din afara Europei. Cu toate acestea, este în interesul strategic al Uniunii să se asigure că păstrează și dezvoltă capacitățile tehnologice esențiale în materie de securitate cibernetică pentru a-și securiza piața unică digitală și, în special, pentru a proteja rețelele și sistemele informatice critice și pentru a furniza servicii de securitate cibernetică esențiale.

(6) Uniunea deține o multitudine de cunoștințe de specialitate și o vastă experiență în ceea ce privește cercetarea, tehnologia și dezvoltarea industrială în materie de securitate cibernetică, însă eforturile comunităților industriale și de cercetare sunt fragmentate, nu există o aliniere între acestea și o misiune comună, fapt care împiedică competitivitatea în acest domeniu. Aceste eforturi și cunoștințe de specialitate trebuie să fie puse în comun, interconectate și utilizate în mod eficient pentru a consolida și a completa capacitățile de cercetare, tehnologice și industriale existente la nivelul Uniunii și la nivel național.

(7) În concluziile sale adoptate în noiembrie 2017, Consiliul a invitat Comisia să prezinte rapid o evaluare a impactului cu privire la opțiunile posibile pentru crearea unei rețele a centrelor de competențe în materie de securitate cibernetică și a unui Centru european de competențe și de cercetare și să propună, până la jumătatea anului 2018, instrumentul juridic relevant.

(8) Centrul de competențe ar trebui să fie principalul instrument de care dispune Uniunea pentru a pune în comun investițiile în cercetarea, tehnologia și dezvoltarea industrială în materie de securitate cibernetică și pentru a pune în aplicare proiectele și inițiativele relevante, împreună cu Rețeaua de competențe în materie de securitate cibernetică. Acesta ar trebui să ofere sprijin financiar în materie de securitate cibernetică din programele Orizont Europa și Europa digitală și ar trebui să fie deschis, după caz, Fondului european de dezvoltare regională și altor programe. Această abordare ar trebui să contribuie la crearea de sinergii și la coordonarea sprijinului financiar pentru cercetarea, inovarea, tehnologia și dezvoltarea industrială în domeniul securității cibernetice și la evitarea suprapunerilor.

(9) Ținând seama de faptul că obiectivele prezentei inițiative pot fi cel mai bine realizate dacă participă toate statele membre sau un număr cât mai mare de state membre și

[22] Comunicare comună către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”, JOIN(2017) 450 final.

pentru a stimula participarea acestora, numai statele membre care contribuie financiar la costurile administrative și operaționale ale Centrului de competențe ar trebui să dețină drepturi de vot.

(10) Participarea financiară a statelor membre participante ar trebui să fie proporțională cu contribuția financiară a Uniunii la această inițiativă.

(11) Centrul de competențe ar trebui să faciliteze și să contribuie la coordonarea activității Rețelei de competențe în materie de securitate cibernetică („rețeaua”), formată din centre naționale de coordonare din fiecare stat membru. Centrele naționale de coordonare ar trebui să beneficieze de sprijin financiar direct din partea Uniunii, inclusiv granturi acordate fără o cerere de propuneri, pentru a desfășura activități legate de prezentul regulament.

(12) Centrele naționale de coordonare ar trebui selectate de către statele membre. Pe lângă capacitatea administrativă necesară, centrele ar trebui fie să dețină, fie să aibă acces direct la expertiză tehnologică în materie de securitate cibernetică, în special în domenii precum criptografia, serviciile de securitate TIC, detectarea intruziunilor, securitatea sistemelor, securitatea rețelelor, securitatea programelor informatice și a aplicațiilor sau aspectele umane și societale ale securității și ale protecției vieții private. Acestea ar trebui, de asemenea, să aibă capacitatea de a-și asuma efectiv angajamente și de a-și coordona acțiunile cu sectorul industrial, cu sectorul public, inclusiv cu autoritățile desemnate în temeiul Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului[23], precum și cu comunitatea de cercetare.

(13) În cazul în care sprijinul financiar este acordat centrelor naționale de coordonare în vederea sprijinirii părților terțe la nivel național, acesta este transferat părților interesate relevante prin acorduri de grant în cascadă.

(14) Tehnologiile emergente, cum ar fi inteligența artificială, internetul obiectelor, calculul de înaltă performanță (HPC) și informatica cuantică, tehnologia blockchain și concepte precum identitățile digitale sigure, creează noi provocări pentru securitatea cibernetică și, în același timp, oferă soluții. Evaluarea și validarea solidității sistemelor TIC existente sau viitoare va necesita testarea soluțiilor de securitate împotriva atacurilor îndreptate împotriva echipamentelor HPC și cuantice. Centrul de competențe, rețeaua și Comunitatea de competențe în materie de securitate cibernetică ar trebui să contribuie la progresul și la diseminarea celor mai recente soluții de securitate cibernetică. În același timp, Centrul de competențe și rețeaua ar trebui să se afle în serviciul dezvoltatorilor și al operatorilor din sectoare critice, cum ar fi transporturile, energia, sănătatea, sectorul financiar, administrația, telecomunicațiile, industria prelucrătoare, apărarea și spațiul, pentru a-i ajuta să își rezolve problemele în materie de securitate cibernetică.

(15) Centrul de competențe ar trebui să dețină mai multe funcții-cheie. În primul rând, acesta ar trebui să faciliteze și să contribuie la coordonarea activității Rețelei europene de competențe în materie de securitate cibernetică și să promoveze Comunitatea de competențe în materie de securitate cibernetică. Centrul ar trebui să promoveze agenda tehnologică în materie de securitate cibernetică și să faciliteze accesul la expertiza acumulată în cadrul rețelei și al Comunității de competențe în materie de securitate

[23] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

cibernetică. În al doilea rând, ar trebui să pună în aplicare părțile relevante din programele Europa digitală și Orizont Europa prin alocarea de granturi, în general în urma unei cereri de propuneri concurențiale. În al treilea rând, centrul de competențe ar trebui să faciliteze investițiile comune din partea Uniunii, a statelor membre și/sau a industriei.

(16) Centrul de competențe ar trebui să stimuleze și să sprijine cooperarea și coordonarea activităților Comunității de competențe în materie de securitate cibernetică, care ar implica un grup mare, deschis și diversificat de actori implicați în tehnologia privind securitatea cibernetică. Această comunitate ar trebui să includă în special entități de cercetare, sectoarele furnizoare, sectoarele cererii, precum și sectorul public. Comunitatea de competențe în materie de securitate cibernetică ar trebui să contribuie la activitățile și la planul de lucru ale Centrului de competențe și ar trebui, de asemenea, să beneficieze de activitățile de consolidare a comunității desfășurate de Centrul de competențe și de rețea, dar nu ar trebui să beneficieze de privilegii în ceea ce privește cererile de propuneri sau procedurile de ofertare.

(17) Pentru a răspunde nevoilor atât ale sectoarelor cererii, cât și ale sectoarelor furnizoare, sarcina Centrului de competențe de a oferi cunoștințe și asistență tehnică în materie de securitate cibernetică pentru aceste sectoare ar trebui să se refere atât la produsele și serviciile TIC, cât și la toate celelalte produse și soluții industriale și tehnologice care ar trebui să includă o componentă de securitate cibernetică.

(18) Având în vedere că Centrul de competențe și rețeaua ar trebui să depună eforturi pentru a realiza sinergii între domeniile civile și de apărare ale securității cibernetice, proiectele finanțate prin programul Orizont Europa vor fi puse în aplicare în conformitate cu Regulamentul XXX [Regulamentul privind programul Orizont Europa], care prevede că activitățile de cercetare și inovare desfășurate în cadrul programului Orizont Europa se concentrează asupra aplicațiilor civile.

(19) Pentru a asigura o colaborare structurată și durabilă, relația dintre Centrul de competențe și centrele naționale de coordonare ar trebui să se bazeze pe un acord contractual.

(20) Ar trebui prevăzute dispoziții adecvate pentru a garanta răspunderea și transparența Centrului de competențe.

(21) Având în vedere expertiza lor în materie de securitate cibernetică, Centrul Comun de Cercetare al Comisiei și Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) ar trebui să joace un rol activ în cadrul Comunității de competențe în materie de securitate cibernetică și al Consiliului consultativ pe probleme industriale și științifice.

(22) În cazul în care primesc o contribuție financiară din bugetul general al Uniunii, centrele naționale de coordonare și entitățile care fac parte din Comunitatea de competențe în materie de securitate cibernetică ar trebui să aducă în atenția publicului faptul că activitățile respective sunt întreprinse în contextul prezentei inițiative.

(23) Contribuția Uniunii la Centrul de competențe ar trebui să finanțeze jumătate din costurile rezultate din activitățile de înființare, administrative și de coordonare ale Centrului de competențe. Pentru a evita dubla finanțare, activitățile respective nu ar trebui să beneficieze simultan de o contribuție din alte programe ale Uniunii.

(24) Consiliul de conducere al Centrului de competențe, alcătuit din reprezentanți ai statelor membre și ai Comisiei, ar trebui să traseze direcția generală de activitate a Centrului de competențe și să se asigure că acesta își îndeplinește sarcinile în

conformitate cu prezentul regulament. Consiliului de conducere ar trebui să i se încredințeze competențele necesare pentru întocmirea bugetului, verificarea execuției acestuia, adoptarea normelor financiare adecvate, stabilirea unor proceduri de lucru transparente pentru luarea deciziilor de către Centrul de competențe, adoptarea planului de lucru și al planului strategic multianual al Centrului de competențe, care reflectă prioritățile în ceea ce privește îndeplinirea obiectivelor și a sarcinilor centrului, adoptarea regulamentului său de procedură, numirea directorului executiv și luarea deciziei cu privire la prelungirea sau încetarea mandatului directorului executiv.

(25) Pentru buna funcționare în condiții de eficacitate a Centrului de competențe, Comisia și statele membre ar trebui să se asigure că persoanele care urmează să fie numite în consiliul de conducere au nivelul adecvat de competență și experiență profesională în domeniile funcționale. Comisia și statele membre ar trebui, de asemenea, să depună eforturi pentru a limita rotația reprezentanților lor în consiliul de conducere, cu scopul de a asigura continuitatea activității acestuia.

(26) Pentru buna funcționare a Centrului de competențe, este necesar ca numirea directorului executiv să fie făcută pe baza meritelor și a aptitudinilor sale administrative și manageriale atestate, precum și a competenței și a experienței relevante în domeniul securității cibernetice și, de asemenea, este necesar ca directorul executiv să își ducă la îndeplinire atribuțiile în deplină independență.

(27) Centrul de competențe ar trebui să aibă drept organism consultativ un Consiliu consultativ pe probleme industriale și științifice, pentru a asigura un dialog regulat cu sectorul privat, cu organizațiile de consumatori și cu alte părți interesate relevante. Consiliul consultativ pe probleme industriale și științifice ar trebui să se concentreze pe chestiunile relevante pentru părțile interesate și să le aducă în atenția consiliului de conducere al Centrului de competențe. Componența Consiliului consultativ pe probleme industriale și științifice și sarcinile care îi revin, cum ar fi consultarea cu privire la planul de lucru, ar trebui să asigure o reprezentare suficientă a părților interesate în activitatea Centrului de competențe.

(28) Centrul de competențe ar trebui să beneficieze de expertiza specifică și de reprezentarea extinsă și relevantă a părților interesate realizată prin intermediul parteneriatului public-privat contractual privind securitatea cibernetică pe durata programului Orizont 2020, prin intermediul Consiliului său consultativ pe probleme industriale și științifice.

(29) Centrul de competențe ar trebui să dispună de norme de prevenire și gestionare a conflictelor de interese. De asemenea, Centrul de competențe ar trebui să aplice dispozițiile relevante ale Uniunii privind accesul public la documente, prevăzute în Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului[24]. Prelucrarea datelor cu caracter personal de către Centrul de competențe face obiectul Regulamentului (UE) nr. XXX/2018 al Parlamentului European și al Consiliului. Centrul de competențe ar trebui să se conformeze dispozițiilor aplicabile instituțiilor Uniunii, precum și dispozițiilor legislațiilor naționale privind gestionarea informațiilor, în special a informațiilor sensibile neclasificate și a informațiilor UE clasificate.

[24] Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).

(30) Interesele financiare ale Uniunii și ale statelor membre ar trebui să fie protejate prin măsuri proporționale pe tot parcursul ciclului de cheltuieli, inclusiv prin prevenirea, depistarea și investigarea neregulilor, prin recuperarea fondurilor pierdute, plătite în mod necuvenit sau incorect utilizate și, dacă este cazul, prin aplicarea de sancțiuni administrative și financiare în conformitate cu Regulamentul XXX (UE, Euratom) al Parlamentului European și al Consiliului[25] [Regulamentul financiar].

(31) Centrul de competențe ar trebui să funcționeze într-un mod deschis și transparent, furnizând toate informațiile relevante în timp util și promovându-și activitățile, inclusiv activitățile de informare și diseminare destinate publicului larg. Regulamentul de procedură al organismelor Centrului de competențe ar trebui să fie pus la dispoziția publicului.

(32) Auditorul intern al Comisiei ar trebui să exercite în cadrul Centrului de competențe aceleași competențe pe care le exercită în cadrul Comisiei.

(33) Comisia, Centrul de competențe, Curtea de Conturi și Oficiul European de Luptă Antifraudă ar trebui să aibă acces la toate informațiile și spațiile de lucru necesare pentru efectuarea de audituri și investigații privind granturile, contractele și acordurile semnate de Centrul de competențe.

(34) Deoarece obiectivele prezentului regulament, și anume menținerea și dezvoltarea capacităților tehnologice și industriale ale Uniunii în materie de securitate cibernetică, creșterea competitivității sectorului securității cibernetice al Uniunii și transformarea securității cibernetice într-un avantaj competitiv al altor sectoare din Uniune, nu pot fi realizate în mod satisfăcător de către statele membre din cauza faptului că resursele limitate existente sunt dispersate, precum și din cauza amplorii investițiilor necesare, ci mai degrabă, pentru a se evita duplicarea inutilă a eforturilor, contribuind la atingerea unei mase critice a investițiilor și garantând utilizarea finanțării publice în cel mai bun mod posibil, pot fi mai bine realizate la nivelul Uniunii, Uniunea poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este definit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea obiectivului respectiv,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

DISPOZIȚII ȘI PRINCIPII GENERALE REFERITOARE LA CENTRUL DE COMPETENȚE ȘI LA REȚEA

Articolul 1

Obiect

1. Prezentul regulament instituie Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică („Centrul de competențe”), precum și Rețeaua de centre naționale de coordonare și stabilește norme pentru numirea centrelor naționale de coordonare, precum și pentru instituirea Comunității de competențe în materie de securitate cibernetică.

[25] [a se adăuga titlul și referința JO]

2. Centrul de competențe contribuie la punerea în aplicare a părții referitoare la securitatea cibernetică din programul Europa digitală, instituit prin Regulamentul nr. XXX și, în special, a acțiunilor legate de articolul 6 din Regulamentul (UE) nr. XXX [programul Europa digitală] din acesta și a programului Orizont Europa, instituit prin Regulamentul nr. XXX și, în special, a secțiunii 2.2.6 din pilonul II al anexei I la Decizia nr. XXX de instituire a programului specific de punere în aplicare a programului-cadru pentru cercetare și inovare Orizont Europa [numărul de referință al programului specific].

3. Centrul de competențe își are sediul la [Bruxelles, Belgia.]

4. Centrul de competențe are personalitate juridică. Acesta dispune, în fiecare stat membru, de cea mai extinsă capacitate juridică acordată persoanelor juridice în temeiul legislației statului membru respectiv. În special, acesta poate să achiziționeze sau să înstrăineze bunuri mobile și imobile și să se constituie parte în proceduri judiciare.

Articolul 2

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

(1) „securitate cibernetică” înseamnă protejarea rețelelor și a sistemelor informatice, a utilizatorilor acestora și a altor persoane împotriva amenințărilor cibernetice;

(2) „produse și soluții de securitate cibernetică” înseamnă produse, servicii sau procese TIC care au drept scop specific protejarea rețelelor și a sistemelor informatice, a utilizatorilor acestora și a altor persoane împotriva amenințărilor cibernetice;

(3) „autoritate publică” înseamnă orice guvern sau altă administrație publică, inclusiv organismele publice consultative, la nivel național, regional sau local sau orice persoană fizică sau juridică ce îndeplinește funcții administrative publice în conformitate cu legislația națională, inclusiv sarcini specifice;

(4) „stat membru participant” înseamnă un stat membru care contribuie financiar în mod voluntar la costurile administrative și operaționale ale Centrului de competențe.

Articolul 3

Misiunea centrului și a rețelei

1. Centrul de competențe și rețeaua ajută Uniunea:

   (a) să mențină și să-și dezvolte capacitățile tehnologice și industriale în materie de securitate cibernetică necesare pentru crearea unei piețe unice digitale sigure;

   (b) să sporească competitivitatea sectorului securității cibernetice al Uniunii și să transforme securitatea cibernetică într-un avantaj competitiv al altor sectoare ale Uniunii.

2. Centrul de competențe își îndeplinește sarcinile, după caz, în colaborare cu Rețeaua de centre naționale de coordonare și cu o Comunitate de competențe în materie de securitate cibernetică.

Articolul 4

Obiectivele și misiunile centrului

Centrul de competențe are următoarele obiective și sarcini conexe:

1. facilitarea și contribuția la coordonarea activității Rețelei de centre naționale de coordonare (denumită în continuare „rețeaua”) menționate la articolul 6 și a Comunității de competențe în materie de securitate cibernetică menționate la articolul 8;

2. contribuția la punerea în aplicare a părții referitoare la securitatea cibernetică din programul Europa digitală, instituit prin Regulamentul nr. XXX[26] și, în special, a acțiunilor legate de articolul 6 din Regulamentul (UE) nr. XXX [programul Europa digitală] și a părții referitoare la securitatea cibernetică din programul Orizont Europa, instituit prin Regulamentul nr. XXX[27] și, în special, a secțiunii 2.2.6 din pilonul II al anexei I la Decizia nr. XXX de instituire a programului specific de punere în aplicare a programului-cadru pentru cercetare și inovare Orizont Europa [numărul de referință al programului specific] și din alte programe ale Uniunii, atunci când acest lucru este prevăzut în actele juridice ale Uniunii;

3. consolidarea capacităților, a cunoștințelor și a infrastructurilor în materie de securitate cibernetică în slujba sectoarelor industriale, a sectorului public și a comunităților de cercetare, prin îndeplinirea următoarelor sarcini:

   (a) având în vedere infrastructurile industriale și de cercetare de ultimă generație în materie de securitate cibernetică și serviciile conexe, achiziționarea, modernizarea, utilizarea și punerea la dispoziție a unor astfel de infrastructuri și servicii conexe pentru o gamă largă de utilizatori din sector din întreaga Uniune, inclusiv IMM-uri, sectorul public și comunitatea științifică și de cercetare;

   (b) având în vedere infrastructurile industriale și de cercetare de ultimă generație în materie de securitate cibernetică și serviciile conexe, oferirea de sprijin, inclusiv de sprijin financiar, altor entități pentru achiziționarea, modernizarea, utilizarea și punerea la dispoziție a unor astfel de infrastructuri și servicii conexe pentru o gamă largă de utilizatori din sector din întreaga Uniune, inclusiv IMM-uri, sectorul public și comunitatea științifică și de cercetare;

   (c) furnizarea de cunoștințe în materie de securitate cibernetică și de asistență tehnică pentru sector și pentru autoritățile publice, în special prin sprijinirea acțiunilor menite să faciliteze accesul la expertiza disponibilă în cadrul rețelei și al Comunității de competențe în materie de securitate cibernetică;

4. contribuția la dezvoltarea pe scară largă a unor produse și soluții de securitate cibernetică de ultimă generație în întreaga economie, prin îndeplinirea următoarelor sarcini:

   (a) stimularea cercetării și dezvoltării legate de produsele și soluțiile de securitate cibernetică ale Uniunii și a adoptării lor de către autoritățile publice și sectoarele utilizatoare;

---

26 [a se adăuga titlul complet și referința JO]

27 [a se adăuga titlul complet și referința JO]

(b) sprijinirea autorităților publice, a sectoarelor cererii și a altor utilizatori în adoptarea și integrarea celor mai recente soluții în materie de securitate cibernetică;

(c) sprijinirea, în special, a autorităților publice în ceea ce privește organizarea achizițiilor lor publice sau efectuarea de achiziții publice de produse și soluții de securitate cibernetică de ultimă generație în numele autorităților publice;

(d) furnizarea de sprijin financiar și de asistență tehnică pentru întreprinderi nou-înființate și IMM-uri din domeniul securității cibernetice pentru a se conecta la piețe potențiale și pentru a atrage investiții;

5. îmbunătățirea înțelegerii securității cibernetice și contribuirea la reducerea lacunelor în materie de competențe din Uniune în ceea ce privește securitatea cibernetică, prin îndeplinirea următoarelor sarcini:

(a) sprijinirea dezvoltării în continuare a competențelor în materie de securitate cibernetică, acolo unde este cazul, împreună cu agențiile și organismele relevante ale UE, inclusiv ENISA.

6. contribuția la consolidarea cercetării și dezvoltării în domeniul securității cibernetice în Uniune prin:

(a) furnizarea de sprijin financiar pentru eforturile de cercetare în materie de securitate cibernetică bazate pe o agendă industrială, tehnologică și de cercetare comună multianuală strategică, evaluată și îmbunătățită în mod continuu, ;

(b) sprijinirea proiectelor de cercetare și demonstrative la scară largă în capacitățile tehnologice de securitate cibernetică de generație următoare, în colaborare cu industria și cu rețeaua;

(c) sprijinirea cercetării și a inovării pentru standardizarea tehnologiei în materie de securitate cibernetică;

7. consolidarea cooperării între domeniile civil și de apărare în ceea ce privește tehnologiile și aplicațiile cu dublă utilizare în materie de securitate cibernetică, prin îndeplinirea următoarelor sarcini:

(a) sprijinirea statelor membre și a părților interesate din sectorul industrial și din domeniul cercetării în ceea ce privește cercetarea, dezvoltarea și implementarea;

(b) contribuția la cooperarea dintre statele membre prin sprijinirea educației, a formării și a exercițiilor;

(c) reunirea părților interesate, pentru a promova sinergiile dintre cercetarea și piețele în materie de securitate cibernetică civile și de apărare;

8. consolidarea sinergiilor dintre dimensiunile civile și cele de apărare ale securității cibernetice în legătură cu Fondul european de apărare, prin îndeplinirea următoarelor sarcini:

(a) furnizarea de consiliere, punerea în comun a expertizei și facilitarea colaborării între părțile interesate relevante;

(b) gestionarea de proiecte multinaționale în domeniul apărării cibernetice, atunci când statele membre solicită acest lucru, acționând astfel în

calitate de manager de proiect în sensul Regulamentului XXX [Regulamentul de instituire a Fondului european de apărare].

Articolul 5

Investiții în infrastructuri, capacități, produse sau soluții și utilizarea acestora

1. În cazul în care Centrul de competențe oferă finanțare pentru infrastructuri, capacități, produse sau soluții în conformitate cu articolul 4 alineatele (3) și (4), sub formă de grant sau de premiu, planul de lucru al Centrului de competențe poate preciza, în special:

   (a) normele care reglementează exploatarea unei infrastructuri sau a unei capacități, inclusiv, după caz, încredințarea acestei sarcini unei entități-gazdă pe baza unor criterii definite de Centrul de competențe;

   (b) normele care reglementează accesul la o infrastructură sau la o capacitate și utilizarea acesteia.

2. Centrul de competențe poate fi responsabil de executarea generală a acțiunilor comune relevante de achiziții publice, inclusiv a achizițiilor înainte de comercializare în numele membrilor rețelei, al membrilor Comunității de competențe în materie de securitate cibernetică sau al altor părți terțe care reprezintă utilizatorii produselor și soluțiilor de securitate cibernetică. În acest scop, Centrul de competențe poate fi asistat de unul sau mai multe centre naționale de coordonare sau de către membri ai Comunității de competențe în materie de securitate cibernetică.

Articolul 6

Desemnarea centrelor naționale de coordonare

1. Până la [data], fiecare stat membru desemnează entitatea care acționează în calitate de centru național de coordonare în sensul prezentului regulament și o notifică Comisiei.

2. Pe baza unei evaluări privind respectarea de către această entitate a criteriilor prevăzute la alineatul (4), Comisia emite o decizie în termen de 6 luni de la desemnarea transmisă de statul membru, prin care acreditează entitatea ca centru național de coordonare sau respinge desemnarea. Lista centrelor naționale de coordonare este publicată de către Comisie.

3. Statele membre pot, în orice moment, să desemneze o nouă entitate în calitate de centru național de coordonare în sensul prezentului regulament. Alineatele (1) și (2) se aplică desemnării oricărei noi entități.

4. Centrul național de coordonare desemnat are capacitatea de a sprijini Centrul de competențe și rețeaua în îndeplinirea misiunii lor prevăzute la articolul 3 din prezentul regulament. Centrele naționale de coordonare dețin sau au acces direct la expertiza tehnologică în materie de securitate cibernetică și sunt în măsură să interacționeze și să se coordoneze în mod eficace cu industria, cu sectorul public și cu comunitatea de cercetare.

5. Relația dintre Centrul de competențe și centrele naționale de coordonare se bazează pe un acord contractual semnat între Centrul de competențe și fiecare dintre centrele naționale de coordonare. Acordul prevede norme care reglementează relația și

repartizarea sarcinilor între Centrul de competențe și fiecare centru național de coordonare.

6. Rețeaua de centre naționale de coordonare este formată din toate centrele naționale de coordonare desemnate de statele membre.

Articolul 7

Sarcinile centrelor naționale de coordonare

1. Centrele naționale de coordonare au următoarele sarcini:

   (a) sprijinirea Centrului de competențe în realizarea obiectivelor sale și, în special, în coordonarea Comunității de competențe în materie de securitate cibernetică;

   (b) facilitarea participării industriei și a altor actori la nivel de stat membru în cadrul proiectelor transfrontaliere;

   (c) contribuția, împreună cu Centrul de competențe, la identificarea și abordarea provocărilor industriale în materie de securitate cibernetică specifice sectorului;

   (d) îndeplinirea rolului de punct de contact la nivel național pentru Comunitatea de competențe în materie de securitate cibernetică și pentru Centrul de competențe;

   (e) stabilirea de sinergii cu activitățile relevante la nivel național și regional;

   (f) punerea în aplicare a acțiunilor specifice pentru care au fost acordate granturi de către Centrul de competențe, inclusiv prin furnizarea de sprijin financiar unor terți în conformitate cu articolul 204 din Regulamentul XXX [noul Regulament financiar] în condițiile specificate în acordurile de grant în cauză;

   (g) promovarea și diseminarea rezultatelor relevante ale activității rețelei, ale Comunității de competențe în materie de securitate cibernetică și ale Centrului de competențe la nivel național sau regional;

   (h) evaluarea cererilor de aderare la Comunitatea de competențe în materie de securitate cibernetică primite din partea entităților stabilite în același stat membru ca centrul de coordonare.

2. În sensul literei (f), sprijinul financiar pentru terți poate fi furnizat în oricare dintre formele specificate la articolul 125 din Regulamentul XXX [noul Regulament financiar], inclusiv sub formă de sume forfetare.

3. Centrele naționale de coordonare pot primi un grant din partea Uniunii în conformitate cu articolul 195 litera (d) din Regulamentul XXX [noul Regulament financiar] în legătură cu îndeplinirea sarcinilor prevăzute în prezentul articol.

4. Centrele naționale de coordonare cooperează, după caz, prin intermediul rețelei în scopul îndeplinirii sarcinilor menționate la alineatul (1) literele (a), (b), (c), (e) și (g).

Articolul 8

Comunitatea de competențe în materie de securitate cibernetică

1. Comunitatea de competențe în materie de securitate cibernetică contribuie la misiunea Centrului de competențe, astfel cum se prevede la articolul 3, și consolidează și disemnează expertiza în materie de securitate cibernetică în întreaga Uniune.

2. Comunitatea de competențe în materie de securitate cibernetică este formată din organizații de cercetare industriale, academice și non-profit, precum și din asociații și entități publice și alte entități care se ocupă de chestiuni operaționale și tehnice. Aceasta reunește principalele părți interesate în ceea ce privește capacitățile tehnologice și industriale în materie de securitate cibernetică din Uniune, implicând centrele naționale de coordonare, precum și instituțiile și organismele Uniunii cu expertiză relevantă.

3. Numai entitățile stabilite în Uniune pot fi acreditate ca membri ai Comunității de competențe în materie de securitate cibernetică. Acestea trebuie să demonstreze că au expertiză în materie de securitate cibernetică în ceea ce privește cel puțin unul dintre următoarele domenii:

   (a) cercetare;

   (b) dezvoltare industrială;

   (c) formare și educație.

4. Centrul de competență acreditează entități instituite în temeiul dreptului național în calitate de membre ale Comunității de competențe în materie de securitate cibernetică în urma unei evaluări efectuate de centrul național de coordonare al statului membru în care este stabilită entitatea, prin care se verifică îndeplinirea de către această entitate a criteriilor prevăzute la alineatul (3). O acreditare nu este limitată în timp, dar poate fi revocată de către Centrul de competențe în orice moment dacă acesta sau centrul național de coordonare consideră că entitatea nu îndeplinește criteriile prevăzute la alineatul (3) sau intră sub incidența dispozițiilor relevante prevăzute la articolul 136 din Regulamentul XXX [noul Regulament financiar].

5. Centrul de competențe acreditează organisme, agenții și oficii relevante ale Uniunii în calitate de membri ai Comunității de competențe în materie de securitate cibernetică după ce a evaluat dacă entitatea în cauză îndeplinește criteriile prevăzute la alineatul (3). O acreditare nu este limitată în timp, dar poate fi revocată de către Centrul de competențe în orice moment în cazul în care consideră că entitatea nu îndeplinește criteriile prevăzute la alineatul (3) sau intră sub incidența dispozițiilor relevante prevăzute la articolul 136 din Regulamentul XXX [noul Regulament financiar].

6. Reprezentanții Comisiei pot participa la activitatea comunității.

Articolul 9

Sarcinile membrilor Comunității de competențe în materie de securitate cibernetică

Membrii Comunității de competențe în materie de securitate cibernetică:

(1) sprijină Centrul de competențe în ceea ce privește îndeplinirea misiunii și a obiectivelor prevăzute la articolele 3 și 4 și, în acest scop, colaborează îndeaproape cu Centrul de competențe și cu centrele naționale de coordonare relevante;

(2) participă la activitățile promovate de Centrul de competențe și de centrele naționale de coordonare;

(3) după caz, participă la grupurile de lucru instituite de consiliul de conducere al Centrului de competențe în vederea desfășurării unor activități specifice, astfel cum se prevede în planul de activitate al Centrului de competențe;

(4) după caz, sprijină Centrul de competențe și centrele naționale de coordonare în promovarea proiectelor specifice;

(5) promovează și difuzează rezultatele relevante ale activităților și proiectelor desfășurate în cadrul comunității.

Articolul 10

Cooperarea Centrului de competențe cu instituțiile, organele, oficiile și agențiile Uniunii

1. Centrul de competențe cooperează cu instituțiile, organele, oficiile și agențiile relevante ale Uniunii, inclusiv cu Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor, cu Centrul de răspuns la incidente de securitate cibernetică (CERT-UE), cu Serviciul European de Acțiune Externă, cu Centrul Comun de Cercetare al Comisiei, cu Agenția Executivă pentru Cercetare, cu Agenția Executivă pentru Inovare și Rețele, cu Centrul european de combatere a criminalității informatice din cadrul Europol, precum și cu Agenția Europeană de Apărare.

2. O astfel de cooperare are loc în cadrul acordurilor de lucru. Aceste acorduri sunt supuse aprobării prealabile a Comisiei.

CAPITOLUL II

ORGANIZAREA CENTRULUI DE COMPETENȚE

Articolul 11

Componență și structură

1. Membrii Centrului de competențe sunt Uniunea, reprezentată de Comisie, și statele membre.

2. Structura Centrului de competențe cuprinde:

(a) un consiliu de conducere, care exercită sarcinile prevăzute la articolul 13;

(b) un director executiv, care exercită sarcinile prevăzute la articolul 16;

(c) un Consiliu consultativ pe probleme industriale și științifice, care exercită funcțiile prevăzute la articolul 20.

SECȚIUNEA I

CONSILIUL DE CONDUCERE

Articolul 12

Componența consiliului de conducere

1. Consiliul de conducere este alcătuit dintr-un reprezentant al fiecărui stat membru și cinci reprezentanți ai Comisiei, în numele Uniunii.

2. Fiecare membru al consiliului de conducere are un supleant care îl reprezintă în absența sa.

3. Membrii consiliului de conducere și supleanții acestora sunt numiți în funcție de cunoștințele lor în domeniul tehnologiei, precum și în funcție de competențele lor manageriale, administrative și bugetare relevante. Comisia și statele membre depun eforturi pentru a limita rotația reprezentanților lor în cadrul consiliului de conducere, cu scopul de a asigura continuitatea activității acestuia. Comisia și statele membre urmăresc realizarea unei reprezentări echilibrate a bărbaților și femeilor în consiliul de conducere.

4. Durata mandatului membrilor consiliului de conducere și al membrilor supleanți este de patru ani. Acest mandat se poate reînnoi.

5. Membrii consiliului de conducere acționează în interesul Centrului de competențe, într-un mod independent și transparent, pentru a îndeplini obiectivele și a realiza misiunea acestuia, asigurându-i identitatea, autonomia și coerența.

6. Comisia poate invita observatori, inclusiv reprezentanți ai unor organisme, oficii și agenții relevante ale Uniunii, să participe la reuniunile consiliului de conducere, dacă este cazul.

7. Agenția Europeană pentru Securitatea Rețelelor și a Informațiilor (ENISA) este observator permanent în consiliul de conducere.

Articolul 13

Sarcinile consiliului de conducere

1. Consiliul de conducere poartă responsabilitatea generală pentru orientarea strategică și operațiunile Centrului de competențe și supraveghează punerea în aplicare a activităților acestuia.

2. Consiliul de conducere își adoptă propriul regulament de procedură. Acest regulament include proceduri specifice pentru identificarea și evitarea conflictelor de interese și pentru asigurarea confidențialității oricăror informații sensibile.

3. Consiliul de conducere ia deciziile strategice necesare, în special:

   (a) adoptă un plan strategic multianual, care conține o declarație privind prioritățile majore și inițiativele planificate ale Centrului de competențe, inclusiv o estimare a nevoilor și a surselor de finanțare;

   (b) adoptă planul de lucru al Centrului de competențe, conturile anuale, bilanțul și raportul anual de activitate, pe baza unei propuneri din partea directorului executiv;

   (c) adoptă normele financiare specifice ale Centrului de competențe, în conformitate cu [articolul 70 din RF];

   (d) adoptă o procedură de numire a directorului executiv;

   (e) adoptă criteriile și procedurile de evaluare și de acreditare a entităților în calitate de membri ai Comunității de competențe în materie de securitate cibernetică;

   (f) desemnează directorul executiv, îl revocă din funcție, îi prelungește mandatul, îi oferă orientări și îi monitorizează activitatea și numește contabilul;

   (g) adoptă bugetul anual al Centrului de competențe, inclusiv schema de personal aferentă, indicând numărul de posturi temporare în funcție de grupa de funcții,

de grad și de numărul membrilor personalului contractual, precum și al experților naționali detașați, exprimat în echivalent normă întreagă;

(h) adoptă norme privind conflictele de interese;

(i) instituie grupuri de lucru cu membrii Comunității de competențe în materie de securitate cibernetică;

(j) numește membrii Consiliului consultativ pe probleme industriale și științifice;

(k) instituie o funcție de audit intern în conformitate cu Regulamentul delegat (UE) nr. 1271/2013 al Comisiei[28];

(l) promovează Centrul de competențe la nivel mondial, astfel încât acesta să își sporească atractivitatea și să devină un organism de talie mondială pentru excelență în materie de securitate cibernetică;

(m) stabilește politica de comunicare a Centrului de competențe, la recomandarea directorului executiv;

(n) este responsabil cu monitorizarea acțiunilor adecvate întreprinse ca urmare a concluziilor evaluărilor retrospective;

(o) după caz, stabilește norme de punere în aplicare a Statutului personalului și a Regimului aplicabil celorlalți agenți în conformitate cu articolul 31 alineatul (3);

(p) după caz, stabilește norme privind detașarea experților naționali la centrul de competențe și recurgerea la stagiari, în conformitate cu articolul 32 alineatul (2);

(q) adoptă de norme de securitate pentru Centrul de competențe;

(r) adoptă o strategie de combatere a fraudei care să fie proporțională cu riscurile de fraudă, ținând seama de analiza cost-beneficiu a măsurilor care ar urma să fie puse în aplicare;

(s) adoptă metodologia de calcul al contribuției financiare din partea statelor membre;

(t) este responsabil cu îndeplinirea oricărei sarcini care nu a fost alocată în mod specific unui anumit organism al Centrului de competențe; poate atribui astfel de sarcini oricărui organism al Centrului de competențe.

Articolul 14

Președintele și reuniunile consiliului de conducere

1. Consiliul de conducere alege un președinte și un vicepreședinte dintre membrii cu drept de vot, pentru o perioadă de doi ani. Mandatul președintelui și al vicepreședintelui poate fi prelungit o singură dată, în urma unei decizii a consiliului de conducere. Cu toate acestea, dacă pe durata mandatului încetează calitatea acestora de membri ai consiliului de conducere, mandatul lor expiră automat la

[28] Regulamentul delegat (UE) nr. 1271/2013 al Comisiei din 30 septembrie 2013 privind regulamentul financiar cadru pentru organismele menționate la articolul 208 din Regulamentul (UE, Euratom) nr. 966/2012 al Parlamentului European și al Consiliului (JO L 328, 7.12.2013, p. 42).

aceeași dată. Vicepreședintele îl înlocuiește din oficiu pe președinte în cazul în care acesta din urmă nu își poate exercita prerogativele. Președintele participă la vot.

2. Consiliul de conducere ține ședințe ordinare de cel puțin trei ori pe an. Acesta poate organiza reuniuni extraordinare la cererea Comisiei, la cererea unei treimi din numărul total al membrilor săi, la cererea președintelui sau la cererea directorului executiv în îndeplinirea sarcinilor sale.

3. Directorul executiv ia parte la deliberări, cu excepția cazului în care consiliul de conducere decide altfel, dar nu are drept de vot. Consiliul de conducere poate invita alte persoane să participe la reuniunile sale în calitate de observatori, de la caz la caz.

4. Membrii Consiliului consultativ pe probleme industriale și științifice pot lua parte la reuniunile consiliului de conducere, la invitația președintelui, fără a avea drept de vot.

5. Sub rezerva propriului regulamentul de procedură, membrii consiliului de conducere și supleanții lor pot să fie asistați în cursul reuniunilor de consilieri sau de experți.

6. Centrul de competențe asigură secretariatul consiliului de conducere.

Articolul 15

Regulile de vot în cadrul consiliului de conducere

1. Uniunea deține 50 % din drepturile de vot. Drepturile de vot ale Uniunii sunt indivizibile.

2. Fiecare stat membru participant deține un vot.

3. Consiliul de conducere adoptă deciziile sale cu o majoritate de cel puțin 75 % din totalul voturilor, inclusiv voturile membrilor care sunt absenți, reprezentând cel puțin 75 % din totalul contribuțiilor financiare către Centrul de competențe. Contribuția financiară va fi calculată pe baza cheltuielilor estimate propuse de statele membre menționate la articolul 17 alineatul (2) litera (c) și pe baza raportului privind valoarea contribuțiilor statelor membre participante menționate la articolul 22 alineatul (5).

4. Numai reprezentanții Comisiei și reprezentanții statelor membre participante dețin drepturi de vot.

5. Președintele participă la vot.

SECȚIUNEA II

DIRECTORUL EXECUTIV

Articolul 16

Numirea, revocarea sau prelungirea mandatului directorului executiv

1. Directorul executiv este o persoană care deține o experiență specifică și o reputație deosebită în domeniile în care își desfășoară activitatea Centrul de competențe.

2. Directorul executiv este angajat ca agent temporar al Centrului de competențe în conformitate cu articolul 2 litera (a) din Regimul aplicabil celorlalți agenți.

3. Directorul executiv este numit de consiliul de conducere dintr-o listă de candidați propuși de Comisie, în urma unei proceduri de selecție deschise și transparente.

4. În scopul încheierii contractului directorului executiv, Centrul de competențe este reprezentat de președintele consiliului de conducere.

5. Durata mandatului directorului executiv este de patru ani. Până la sfârșitul perioadei respective, Comisia realizează o analiză care ia în considerare evaluarea rezultatelor obținute de directorul executiv și viitoarele sarcini și provocări cu care se va confrunta Centrul de competențe.

6. La propunerea Comisiei, care ia în considerare evaluarea menționată la alineatul (5), consiliul de conducere poate reînnoi mandatul directorului executiv o singură dată, cu cel mult patru ani.

7. Un director executiv al cărui mandat a fost prelungit nu poate să participe la o nouă procedură de selecție pentru același post.

8. Directorul executiv este demis din funcție numai printr-o decizie a consiliului de conducere, care acționează la propunerea Comisiei.

Articolul 17

Sarcinile directorului executiv

1. Directorul executiv este responsabil de operațiuni și de gestionarea curentă a Centrului de competențe și este reprezentantul legal al acestuia. Directorul executiv răspunde în fața consiliului de conducere și își execută atribuțiile în deplină independență, în limita prerogativelor acordate.

2. Directorul executiv îndeplinește în special următoarele sarcini în mod independent:

   (a) punerea în aplicare a deciziilor adoptate de consiliul de conducere;

   (b) sprijinirea activităților consiliului de conducere, asigurarea secretariatului reuniunilor acestuia și furnizarea tuturor informațiilor necesare pentru îndeplinirea sarcinilor acestuia;

   (c) după consultarea consiliului de conducere și a Comisiei, pregătirea și înaintarea spre adoptare consiliului de conducere a proiectului de plan strategic multianual și a proiectului de plan anual de activitate ale Centrului de competențe, inclusiv obiectul cererilor de propuneri, al cererilor de exprimare a interesului și al cererilor de oferte necesare pentru punerea în aplicare a planului de lucru și a estimărilor privind cheltuielile aferente, astfel cum au fost propuse de statele membre și de Comisie;

   (d) pregătirea și înaintarea spre adoptare consiliului de conducere a proiectului de buget anual, inclusiv a schemei de personal aferente, care indică numărul de posturi temporare în fiecare grad și grupă de funcții, precum și numărul de agenți contractuali și de experți naționali detașați, exprimat în echivalent normă întreagă;

   (e) punerea în aplicare a planului de lucru și prezentarea de rapoarte către consiliul de conducere;

   (f) pregătirea proiectului de raport anual de activitate al Centrului de competențe, inclusiv prezentarea de informații privind cheltuielile aferente;

   (g) asigurarea punerii în aplicare a unor proceduri eficiente de monitorizare și de evaluare a performanțelor Centrului de competențe;

   (h) pregătirea unui plan de acțiune pentru a da curs concluziilor evaluărilor retrospective și trimiterea către Comisie, la fiecare doi ani, a unui raport privind progresele înregistrate;

(i) pregătirea, negocierea și încheierea de acorduri cu centrele naționale de coordonare;

(j) este responsabil de aspectele administrative, financiare și de personal, inclusiv de execuția bugetului Centrului de competențe, ținând seama în mod corespunzător de recomandările primite din partea funcției de audit intern, în limitele delegării conferite de către consiliul de conducere;

(k) aprobarea și gestionarea lansării cererilor de propuneri, în conformitate cu planul de lucru, și administrarea acordurilor și a deciziilor de grant;

(l) aprobarea listei de acțiuni selectate pentru finanțare pe baza clasamentului stabilit de un grup de experți independenți;

(m) aprobarea și gestionarea lansării procedurilor de ofertare, în conformitate cu planul de lucru, și administrarea contractelor;

(n) aprobarea ofertelor selectate pentru finanțare;

(o) prezentarea proiectului de conturi anuale și a proiectului de bilanț anual funcției de audit intern și, ulterior, consiliului de conducere;

(p) asigurarea efectuării evaluării și a gestionării riscurilor;

(q) semnarea acordurilor, deciziilor și contractelor individuale de grant;

(r) semnarea contractelor de achiziții;

(s) elaborarea unui plan de acțiune în urma concluziilor rapoartelor de audit intern sau extern, precum și a investigațiilor desfășurate de Oficiul European de Luptă Antifraudă (OLAF) și prezentarea, de două ori pe an Comisiei și periodic consiliului de conducere, a unui raport privind progresele înregistrate;

(t) elaborarea proiectului de reguli financiare aplicabile Centrului de competențe;

(u) stabilirea și asigurarea funcționării unui sistem de control intern eficace și eficient și raportarea către consiliul de conducere a oricărei modificări semnificative a acestuia;

(v) asigurarea unei comunicări eficiente cu instituțiile Uniunii;

(w) adoptarea oricărei alte măsuri necesare pentru a evalua progresul Centrului de competențe în ceea ce privește misiunea și obiectivele acestuia, astfel cum se prevede la articolele 3 și 4 din prezentul regulament;

(x) executarea oricărei alte sarcini care îi este atribuită sau delegată de consiliul de conducere.

SECȚIUNEA III

CONSILIUL CONSULTATIV PE PROBLEME INDUSTRIALE ȘI ȘTIINȚIFICE

Articolul 18

Structura Consiliului consultativ pe probleme industriale și științifice

1. Consiliul consultativ pe probleme industriale și științifice este format din cel mult 16 membri. Membrii sunt numiți de consiliul de conducere dintre reprezentanții entităților din cadrul Comunității de competențe în materie de securitate cibernetică.

2. Membrii Consiliului consultativ pe probleme industriale și științifice dețin competențe specifice în ceea ce privește cercetarea în domeniul securității

cibernetice, dezvoltarea industrială, serviciile profesionale sau desfășurarea acestora. Cerințele pentru astfel de competențe specifice sunt precizate în detaliu de către consiliul de conducere.

3. Procedurile privind numirea membrilor săi de către consiliul de conducere și funcționarea Consiliului consultativ sunt precizate în regulamentul de procedură al Centrului de competențe și sunt făcute publice.

4. Durata mandatului membrilor Consiliului consultativ pe probleme industriale și științifice este de trei ani Acest mandat se poate reînnoi.

5. Reprezentanții Comisiei și ai Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor pot participa la lucrările Consiliului consultativ pe probleme industriale și științifice și pot sprijini lucrările acestuia.

Articolul 19

Funcționarea Consiliului consultativ pe probleme industriale și științifice

1. Consiliul consultativ pe probleme industriale și științifice se întrunește cel puțin de două ori pe an.

2. Consiliul consultativ pe probleme industriale și științifice poate oferi consiliere consiliului de conducere cu privire la instituirea de grupuri de lucru cu privire la aspecte specifice relevante pentru activitatea Centrului de competențe, atunci când acest lucru este necesar în cadrul coordonării generale a unuia sau mai multor membri ai Consiliului consultativ pe probleme industriale și științifice.

3. Consiliul consultativ pe probleme industriale și științifice își alege președintele.

4. Consiliul consultativ pe probleme industriale și științifice își adoptă regulamentul de procedură, inclusiv îi desemnează pe reprezentanții Consiliului consultativ, după caz, și stabilește durata mandatului acestora.

Articolul 20

Sarcinile Consiliului consultativ pe probleme industriale și științifice

Consiliul consultativ pe probleme industriale și științifice informează Centrul de competențe cu privire la desfășurarea activităților sale și:

(1) oferă directorului executiv și consiliului de conducere consiliere strategică și contribuții la elaborarea planului de lucru și a planului strategic multianual în termenele stabilite de consiliul de conducere;

(2) organizează consultări publice deschise tuturor părților interesate din sectorul public și privat care au un interes în domeniul securității cibernetice, pentru a colecta contribuții pentru consilierea strategică menționată la alineatul (1);

(3) promovează și colectează feedback cu privire la planul de lucru și la planul strategic multianual ale Centrului de competențe.

CAPITOLUL III
DISPOZIȚII FINANCIARE

Articolul 21

Contribuția financiară a Uniunii

1. Contribuția Uniunii la centrul de competențe pentru acoperirea costurilor administrative și a costurilor operaționale cuprinde următoarele:

   (a) 1 981 668 000 EUR din programul Europa digitală, inclusiv până la 23 746 000 EUR pentru costuri administrative;

   (b) O sumă din programul Orizont Europa, inclusiv în ceea ce privește costurile administrative, care urmează să fie stabilită ținând seama de procesul de planificare strategică care va fi efectuat în conformitate cu articolul 6 alineatul (6) din Regulamentul XXX [Regulamentul privind programul Orizont Europa].

2. Contribuția maximă a Uniunii se plătește din creditele din bugetul general al Uniunii alocate pentru [programul Europa digitală] și din creditele alocate programului specific de punere în aplicare a programului Orizont Europa, instituit prin Decizia XXX.

3. Centrul de competențe pune în aplicare acțiunile în materie de securitate cibernetică ale [programului Europa digitală] și ale [programului Orizont Europa] în conformitate cu articolul 62 litera (c) punctul (iv) din Regulamentul (UE, Euratom) XXX[29] [Regulamentul financiar].

4. Contribuția financiară a Uniunii nu acoperă sarcinile menționate la articolul 4 alineatul (8) litera (b).

Articolul 22

Contribuțiile statelor membre participante

1. Statele membre participante au o contribuție totală la costurile operaționale și administrative ale Centrului de competențe cel puțin egală cu cea prevăzută la articolul 21 alineatul (1) din prezentul regulament.

2. În scopul evaluării contribuțiilor menționate la alineatul (1) și la articolul 23 alineatul (3) litera (b) punctul (ii), costurile se stabilesc în conformitate cu practicile obișnuite de contabilitate a costurilor ale statelor membre în cauză, cu standardele de contabilitate aplicabile ale statului membru și cu standardele internaționale de contabilitate și standardele internaționale de raportare financiară aplicabile. Costurile sunt certificate de un auditor extern independent desemnat de statul membru în cauză. Metoda de evaluare poate fi verificată de către Centrul de competențe, în cazul în care există dubii cu privire la certificare.

3. Dacă un stat membru participant nu își îndeplinește angajamentele privind contribuția sa financiară, directorul executiv consemnează acest lucru și stabilește un termen rezonabil pentru remedierea acestei situații. Dacă situația nu este remediată în termenul respectiv, directorul executiv convoacă o reuniune a consiliului de

[29] [a se adăuga titlul complet și referința JO]

conducere pentru a decide dacă dreptul de vot al statului membru participant care nu și-a îndeplinit obligațiile trebuie revocat sau dacă trebuie luate alte măsuri până la îndeplinirea obligațiilor de către acesta. Drepturile de vot ale statului membru care nu și-a îndeplinit obligațiile sunt suspendate până la remedierea situației.

4. Comisia poate suprima, reduce în mod proporțional sau suspenda contribuția financiară a Uniunii către Centrul de competențe în cazul în care statele membre participante nu efectuează, efectuează doar parțial sau efectuează cu întârziere contribuțiile menționate la alineatul (1).

5. Până la data de 31 ianuarie a fiecărui an, statele membre participante prezintă un raport consiliului de conducere cu privire la valoarea contribuțiilor menționate la alineatul (1), efectuate în fiecare dintre exercițiile financiare precedente.

Articolul 23

Costurile și resursele centrului de competențe

1. Centrul de competențe este finanțat în comun de Uniune și de statele membre prin contribuții financiare plătite în tranșe și contribuții aferente costurilor suportate de centrele naționale de coordonare și de beneficiari în cadrul punerii în aplicare a unor acțiuni care nu sunt rambursate de către Centrul de competențe.

2. Costurile administrative ale Centrului de competențe nu depășesc [număr] EUR și sunt acoperite prin contribuții financiare anuale, divizate în mod egal între Uniune și statele membre participante. În cazul în care o parte din contribuția la costurile administrative nu este utilizată, aceasta poate fi pusă la dispoziție pentru acoperirea costurilor operaționale ale Centrului de competențe.

3. Costurile operaționale ale Centrului de competențe sunt acoperite prin:

   (a) contribuția financiară a Uniunii;

   (b) contribuții din partea statelor membre participante sub formă de:

      (i) contribuții financiare; și

      (ii) după caz, contribuții în natură ale statelor membre participante la costurile suportate de centrele naționale de coordonare și de beneficiari în cadrul punerii în aplicare a acțiunilor indirecte, din care se scade contribuția Centrului de competențe și orice altă contribuție a Uniunii la aceste costuri;

4. Resursele centrului de competențe incluse în bugetul acestuia constau în următoarele contribuții:

   (a) contribuții financiare ale statelor membre participante la costurile administrative;

   (b) contribuții financiare ale statelor membre participante la costurile operaționale;

   (c) orice venituri generate de Centrul de competențe;

   (d) orice alte contribuții financiare, resurse și venituri.

5. Orice dobândă generată de contribuțiile plătite Centrului de competențe de către statele membre participante este considerată drept venit al acestuia.

6. Toate resursele Centrului de competențe și activitățile acestuia au ca scop îndeplinirea obiectivelor prevăzute la articolul 4.

7. Centrul de competențe este proprietarul tuturor activelor generate de el sau transferate către el în scopul îndeplinirii obiectivelor sale.

8. Cu excepția situației de lichidare a Centrului de competențe, orice excedent de venit în raport cu cheltuielile nu se plătește membrilor participanți ai Centrului de competențe.

Articolul 24

Angajamente financiare

Angajamentele financiare ale Centrului de competențe nu depășesc valoarea totală a resurselor financiare disponibile sau angajate la buget de către membrii acestuia.

Articolul 25

Exercițiul financiar

Exercițiul financiar începe la 1 ianuarie și se încheie la 31 decembrie.

Articolul 26

Întocmirea bugetului

1. În fiecare an, directorul executiv elaborează un proiect de situație a estimărilor de venituri și cheltuieli ale Centrului de competențe pentru următorul exercițiu financiar și îl înaintează consiliului de conducere, împreună cu un proiect de schemă de personal. Veniturile și cheltuielile trebuie să fie în echilibru. Cheltuielile Centrului de competențe cuprind cheltuielile cu personalul, cheltuielile administrative, cheltuielile de infrastructură și cheltuielile operaționale. Cheltuielile administrative sunt menținute la minimum.

2. În fiecare an, pe baza proiectului situației estimărilor de venituri și cheltuieli menționat la alineatul (1), consiliul de conducere adoptă situația estimărilor de venituri și cheltuieli ale Centrului de competențe pentru următorul exercițiu financiar.

3. În fiecare an, până la data de 31 ianuarie, consiliul de conducere transmite Comisiei situația estimărilor menționată la alineatul (2), care face parte din documentul unic de programare.

4. Pe baza situației estimărilor respective, Comisia înscrie în proiectul de buget al Uniunii estimările pe care le consideră necesare pentru schema de personal și valoarea contribuției care urmează să fie suportată din bugetul general, pe care le prezintă Parlamentului European și Consiliului în conformitate cu articolele 313 și 314 din TFUE.

5. Parlamentul European și Consiliul autorizează creditele reprezentând contribuția alocată Centrului de competențe.

6. Parlamentul European și Consiliul adoptă schema de personal a Centrului de competențe.

7. Consiliul de conducere adoptă bugetul centrului odată cu planul de lucru. Bugetul centrului devine definitiv după adoptarea definitivă a bugetului general al Uniunii. După caz, consiliul de conducere ajustează bugetul Centrului de competențe și planul de lucru în conformitate cu bugetul general al Uniunii.

Articolul 27

Prezentarea conturilor Centrului de competențe și descărcarea de gestiune

Prezentarea conturilor provizorii și finale ale Centrului de competențe și descărcarea de gestiune respectă normele și calendarul Regulamentului financiar și ale normelor financiare ale acestuia, adoptate în conformitate cu articolul 29.

Articolul 28

Raportarea operațională și financiară

1. Directorul executiv prezintă anual consiliului de conducere un raport referitor la executarea sarcinilor sale în conformitate cu normele financiare ale Centrului de competențe.

2. În termen de două luni de la încheierea fiecărui exercițiu financiar, directorul executiv prezintă consiliului de conducere spre aprobare un raport anual de activitate referitor la progresul înregistrat de Centrul de competențe în anul calendaristic anterior, în special în ceea ce privește planul de lucru pentru anul respectiv. Raportul include, printre altele, informații cu privire la următoarele aspecte:

   (a) acțiunile operaționale desfășurate și cheltuielile aferente;

   (b) acțiunile prezentate, inclusiv o defalcare în funcție de tipul de participant, inclusiv IMM-uri, și în funcție de statul membru;

   (c) acțiunile selectate pentru finanțare, inclusiv o defalcare în funcție de tipul de participant, inclusiv IMM-uri, și n funcție de statul membru, cu indicarea contribuției Centrului de competențe destinate participanților individuali și acțiunilor individuale;

   (d) progresele înregistrate în privința atingerii obiectivelor prevăzute la articolul 4 și propuneri de alte acțiuni necesare în vederea îndeplinirii acestor obiective.

3. După aprobarea sa de către consiliul de conducere, raportul anual de activitate este pus la dispoziția publicului.

Articolul 29

Regulile financiare

Centrul de competențe își adoptă normele financiare specifice în conformitate cu articolul 70 din Regulamentul XXX [noul Regulament financiar].

Articolul 30

Protejarea intereselor financiare

1. În cursul punerii în aplicare a acțiunilor finanțate în temeiul prezentului regulament, Centrul de competențe ia măsurile corespunzătoare care să garanteze protejarea intereselor financiare ale Uniunii prin aplicarea de măsuri preventive împotriva fraudei, corupției și a oricăror alte activități ilegale, prin controale eficace și, în cazul în care se constată nereguli, prin recuperarea sumelor plătite în mod necuvenit, precum și, dacă este necesar, prin sancțiuni administrative eficace, proporționale și disuasive.

2. Centrul de competențe acordă personalului Comisiei și altor persoane autorizate de Comisie, precum și Curții de Conturi, acces la sediile și spațiile sale și la toate informațiile necesare pentru efectuarea auditurilor acestora, inclusiv la informațiile în format electronic.

3. Oficiul European de Luptă Antifraudă (OLAF) poate efectua investigații, inclusiv verificări și inspecții la fața locului, în conformitate cu dispozițiile și procedurile prevăzute în Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului[30] și în Regulamentul (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului[31], cu scopul de a stabili existența unei fraude, a unui act de corupție sau dacă a avut loc orice altă activitate ilegală care afectează interesele financiare ale Uniunii în legătură cu un acord de grant sau cu un contract finanțat, direct sau indirect, în conformitate cu prezentul regulament.

4. Fără a aduce atingere alineatelor (1), (2) și (3) din prezentul articol, contractele și acordurile de grant care rezultă din punerea în aplicare a prezentului regulament conțin dispoziții care împuternicesc în mod expres Comisia, Centrul de competențe, Curtea de Conturi și OLAF să efectueze astfel de audituri și investigații, în conformitate cu competențele acestora. În cazul în care punerea în aplicare a unei acțiuni este externalizată sau subdelegată, în totalitate sau parțial, sau în cazul în care se impune atribuirea unui contract de achiziții publice sau de sprijin financiar unui terț, contractul sau acordul de grant include obligația contractantului sau a beneficiarului de a impune oricărei părți terțe implicate acceptarea explicită a acestor competențe ale Comisiei, ale Centrului de competențe, ale Curții de Conturi și ale OLAF.

CAPITOLUL IV
PERSONALUL CENTRULUI DE COMPETENȚE

Articolul 31

Personalul

1. Statutul funcționarilor și Regimul aplicabil celorlalți agenți ai Uniunii Europene, astfel cum sunt stabilite în Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului[32] (denumite în continuare „Statutul funcționarilor” și „Regimul aplicabil celorlalți agenți”) și normele adoptate în comun de instituțiile Uniunii în scopul aplicării Statutului funcționarilor și a Regimului aplicabil celorlalți agenți se aplică personalului Centrului de competențe.

---

30 Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului din 11 noiembrie 1996 privind controalele și inspecțiile la fața locului efectuate de Comisie în scopul protejării intereselor financiare ale Comunităților Europene împotriva fraudei și a altor abateri (JO L 292, 15.11.1996, p. 2).

31 Regulamentul (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului din 11 septembrie 2013 privind investigațiile efectuate de Oficiul European de Luptă Antifraudă (OLAF) și de abrogare a Regulamentului (CE) nr. 1073/1999 al Parlamentului European și al Consiliului și a Regulamentului (Euratom) nr. 1074/1999 al Consiliului (JO L 248, 18.9.2013, p. 1).

32 Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului din 29 februarie 1968 de stabilire a Statutului funcționarilor Comunităților Europene, precum și a Regimului aplicabil celorlalți agenți ai acestor comunități și de instituire a unor măsuri speciale tranzitorii aplicabile funcționarilor Comisiei (JO L 56, 4.3.1968, p. 1).

2. Consiliul de conducere exercită, în ceea ce privește personalul Centrului de competențe, competențele conferite autorității de numire prin Statutul funcționarilor și competențele conferite autorității abilitate să încheie contracte prin Regimul aplicabil celorlalți agenți (denumite în continuare „competențele autorității de numire”).

3. Consiliul de conducere adoptă, în conformitate cu articolul 110 din Statutul funcționarilor, o decizie, în temeiul articolului 2 alineatul (1) din Statutul funcționarilor și al articolului 6 din Regimul aplicabil celorlalți agenți, prin care competențele relevante ale autorității de numire sunt delegate directorului executiv și în care sunt definite condițiile în care această delegare de competențe poate fi suspendată. Directorul executiv este autorizat să subdelege competențele respective.

4. În cazul în care anumite circumstanțe excepționale impun acest lucru, consiliul de conducere poate, printr-o decizie, să suspende temporar delegarea competențelor autorității de numire către directorul executiv, precum și orice subdelegare efectuată de către acesta. În acest caz, consiliul de conducere exercită el însuși competențele autorității de numire sau le deleagă unuia dintre membrii săi sau unui membru al personalului centrului de competențe, altul decât directorul executiv.

5. Consiliul de conducere adoptă norme de punere în aplicare referitoare la Statutul funcționarilor și la Regimul aplicabil celorlalți agenți, în conformitate cu articolul 110 din Statutul funcționarilor.

6. Resursele de personal sunt stabilite în schema de personal a Centrului de competențe, indicându-se numărul de posturi temporare pe grupe de funcții și pe grade, precum și numărul de agenți contractuali, exprimat în echivalent normă întreagă, în conformitate cu bugetul anual al acestuia.

7. Personalul centrului de competențe este format din agenți temporari și agenți contractuali.

8. Toate costurile cu privire la personal sunt suportate de Centrul de competențe.

Articolul 32

Experți naționali detașați și alte categorii de personal

1. Centrul de competențe poate recurge la experți naționali detașați sau alte categorii de personal care nu sunt angajați ai Centrului de competențe.

2. Consiliul de conducere adoptă o decizie de stabilire a normelor aplicabile detașării experților naționali la Centrul de competențe, de comun acord cu Comisia.

Articolul 33

Privilegii și imunități

Centrului de competențe și personalului acestuia li se aplică Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene.

CAPITOLUL V
DISPOZIȚII COMUNE

Articolul 34

Norme de securitate

1. Articolul 12 alineatul (7) din Regulamentul (UE) nr. XXX [programul Europa digitală] se aplică participării la toate acțiunile finanțate de Centrul de competențe.

2. Următoarele norme de securitate specifice se aplică acțiunilor finanțate din programul Orizont Europa:

   (a) în sensul articolului 34 alineatul (1) [Proprietate și protecție] din Regulamentul (UE) nr. XXX [Orizont Europa], atunci când planul de lucru prevede acest lucru, acordarea de licențe neexclusive poate fi limitată la terți stabiliți sau considerați a fi stabiliți în statele membre și controlați de state membre și/sau de resortisanți ai statelor membre;

   (b) în sensul articolului 36 alineatul (4) litera (b) [Transfer și acordarea de licențe] din Regulamentul (UE) nr. XXX [Orizont Europa], transferul sau acordarea de licență către o entitate juridică stabilită într-o țară asociată sau stabilită în Uniune, dar controlată din țări terțe este, de asemenea, un motiv pentru a se opune transferului de proprietate asupra rezultatelor sau acordării unei licențe exclusive cu privire la rezultate;

   (c) în sensul articolului 37 alineatul (3) litera (a) [Drepturi de acces] din Regulamentul (UE) nr. XXX [Orizont Europa], atunci când planul de lucru prevede acest lucru, acordarea accesului la rezultate și la informațiile preexistente poate fi limitată doar la o entitate juridică stabilită sau considerată a fi stabilită în statele membre și controlată de statele membre și/sau de resortisanți ai statelor membre.

Articolul 35

Transparență

1. Centrul de competențe își desfășoară activitățile cu un nivel ridicat de transparență.

2. Centrul de competențe se asigură că publicului și tuturor părților interesate li se furnizează informații adecvate, obiective, fiabile și ușor accesibile, în special în ceea ce privește rezultatele activității sale. De asemenea, acesta face publice declarațiile de interese întocmite în conformitate cu articolul 41.

3. Consiliul de conducere, pe baza unei propuneri primite de la directorul executiv, poate autoriza părțile interesate să participe ca observatori la unele dintre activitățile Centrului de competențe.

4. Centrul de competențe stabilește, în regulamentul său de procedură, modalitățile practice de punere în aplicare a normelor privind transparența menționate la alineatele (1) și (2). În cazul acțiunilor finanțate din programul Orizont Europa, se va ține seama în mod corespunzător de dispozițiile anexei III la Regulamentul privind programul Orizont Europa.

Articolul 36

Norme de securitate privind protejarea informațiilor clasificate și a informațiilor sensibile neclasificate

1. Fără a aduce atingere articolului 35, Centrul de competențe nu divulgă terților informațiile pe care le prelucrează sau pe care le primește și pentru care s-a cerut, printr-o solicitare motivată, un tratament confidențial, integral sau parțial.

2. Membrii consiliului de conducere, directorul executiv, membrii Consiliul consultativ pe probleme industriale și științifice, experții externi care participă la grupurile de lucru ad-hoc și membrii personalului centrului respectă cerințele de confidențialitate prevăzute la articolul 339 din Tratatul privind funcționarea Uniunii Europene, chiar și după încetarea atribuțiilor lor.

3. Consiliul de conducere al Centrului de competențe adoptă normele de securitate ale Centrului de competențe, după aprobarea de către Comisie, pe baza principiilor și a normelor stabilite în normele de securitate ale Comisiei pentru protecția informațiilor UE clasificate (IUEC) și a informațiilor sensibile neclasificate, inclusiv, inter alia, dispoziții privind prelucrarea și stocarea informațiilor respective, astfel cum se prevede în Deciziile (UE, Euratom) 2015/443[33] și 2015/444[34] ale Comisiei.

4. Centrul de competențe poate lua toate măsurile necesare în vederea facilitării schimbului de informații relevante pentru sarcinile sale cu Comisia și statele membre și, acolo unde este cazul, cu agențiile și organismele relevante ale Uniunii. Orice acord administrativ încheiat în acest scop cu privire la partajarea IUEC sau, în absența unui astfel de acord, orice comunicare excepțională ad-hoc a IUEC trebuie să primească aprobarea prealabilă a Comisiei.

Articolul 37

Accesul la documente

1. Regulamentul (CE) nr. 1049/2001 se aplică documentelor deținute de Centrul de competențe.

2. Consiliul de conducere adoptă modalitățile de punere în aplicare a Regulamentului (CE) nr. 1049/2001 în termen de șase luni de la înființarea Centrului de competențe.

3. Deciziile adoptate de Centrul de competențe în temeiul articolului 8 din Regulamentul (CE) nr. 1049/2001 pot face obiectul unei plângeri adresate Ombudsmanului în temeiul articolului 228 din Tratatul privind funcționarea Uniunii Europene sau al unei acțiuni înaintate Curții de Justiție a Uniunii Europene în temeiul articolului 263 din Tratatul privind funcționarea Uniunii Europene.

Articolul 38

Monitorizare, evaluare și revizuire

---

33 Decizia (UE, Euratom) 2015/443 a Comisiei din 13 martie 2015 privind securitatea în cadrul Comisiei (JO L 72, 17.3.2015, p. 41).

34 Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 72, 17.3.2015, p. 53).

1. Centrul de competențe se asigură că activitățile sale, inclusiv cele gestionate prin intermediul centrelor naționale de coordonare și al rețelei, fac obiectul monitorizării continue și sistematice și al evaluării periodice. Centrul de competențe se asigură că datele pentru monitorizarea punerii în aplicare și a rezultatelor programului sunt colectate în mod eficient, eficace și în timp util și că se impun cerințe de raportare proporționale pentru beneficiarii fondurilor Uniunii și pentru statele membre. Rezultatele evaluării se fac publice.

2. Odată ce există suficiente informații disponibile cu privire la punerea în aplicare a prezentului regulament, dar nu mai târziu de trei ani și jumătate de la începerea punerii sale în aplicare, Comisia efectuează o evaluare intermediară a centrului de competențe. Comisia întocmește un raport cu privire la această evaluare și transmite raportul respectiv Parlamentului European și Consiliului până la 31 decembrie 2024. Centrul de competențe și statele membre furnizează Comisiei informațiile necesare pentru pregătirea respectivului raport.

3. Evaluarea menționată la alineatul (2) include o evaluare a rezultatelor obținute de către Centrul de competențe, având în vedere obiectivele, mandatul și sarcinile sale. În cazul în care consideră că existența Centrului de competențe este în continuare justificată în raport cu obiectivele, mandatul și sarcinile acestuia, Comisia poate propune ca durata mandatului Centrului de competențe, prevăzută la articolul 46, să fie prelungită.

4. Pe baza concluziilor evaluării intermediare menționate la alineatul (2), Comisia poate acționa în conformitate cu [articolul 22 alineatul (5)] sau poate lua orice altă măsură adecvată.

5. Monitorizarea, evaluarea, eliminarea treptată și reînnoirea contribuției din partea programului Orizont Europa vor respecta dispozițiile articolelor 8, 45 și 47 și ale anexei III din Regulamentul privind programul Orizont Europa și modalitățile de punere în aplicare convenite.

6. Monitorizarea, raportarea și evaluarea contribuției din partea programului Europa digitală vor respecta dispozițiile articolelor 24 și 25 din programul Europa digitală.

7. În cazul lichidării Centrului de competențe, Comisia efectuează o evaluare finală a Centrului de competențe în termen de șase luni de la lichidarea acestuia, dar nu mai târziu de doi ani de la declanșarea procedurii de lichidare menționate la articolul 46 din prezentul regulament. Rezultatele evaluării finale sunt prezentate Parlamentului European și Consiliului.

Articolul 39

Răspunderea Centrului de competențe

1. Răspunderea contractuală a Centrului de competențe este reglementată de dreptul aplicabil acordului, deciziei sau contractului în cauză.

2. În cazul răspunderii extracontractuale, în conformitate cu principiile generale comune legislațiilor statelor membre, Centrul de competențe acordă despăgubiri pentru toate prejudiciile provocate de personalul său în exercițiul funcțiunii.

3. Orice plată efectuată de Centrul de competențe destinată să acopere răspunderea menționată la alineatele (1) și (2), precum și costurile și cheltuielile aferente sunt considerate cheltuieli ale Centrului de competențe și sunt suportate din resursele acestuia.

4. Centrul de competențe este singurul responsabil pentru îndeplinirea obligațiilor sale.

Articolul 40

Competența Curții de Justiție a Uniunii Europene și dreptul aplicabil

1. Curtea de Justiție a Uniunii Europene are competențe:

   (1) în temeiul unei clauze compromisorii prevăzute în acordurile, deciziile sau contractele încheiate de Centrul de competențe;

   (2) în litigiile referitoare la despăgubirile acordate pentru prejudiciile cauzate de personalul Centrului de competențe în exercițiul funcțiunii sale;

   (3) în litigiile dintre Centrul de competențe și personalul său în limitele și condițiile prevăzute de Statutul funcționarilor.

2. Pentru orice aspect care nu este reglementat prin prezentul regulament sau prin alte acte juridice ale Uniunii, se aplică legislația statului membru în care se află sediul Centrului de competențe.

Articolul 41

Răspunderea membrilor și asigurarea

1. Răspunderea financiară a membrilor în ceea ce privește datoriile Centrului de competențe se limitează la contribuția lor deja plătită în contul cheltuielilor administrative.

2. Centrul de competențe subscrie la o asigurare adecvată și efectuează plățile necesare.

Articolul 42

Conflicte de interese

Consiliul de conducere al Centrului de competențe adoptă norme pentru prevenirea și gestionarea conflictelor de interese în rândul membrilor, organismelor și personalului acesteia. Aceste norme conțin dispozițiile menite să evite un conflict de interese în ceea ce privește reprezentanții membrilor care fac parte din consiliul de conducere, precum și din Consiliul consultativ pe probleme industriale și științifice, în conformitate cu Regulamentul XXX [noul Regulament financiar].

Articolul 43

Protecția datelor cu caracter personal

1. Prelucrarea datelor cu caracter personal de către Centrul de competențe face obiectul Regulamentului (UE) nr. XXX/2018 al Parlamentului European și al Consiliului.

2. Consiliul de conducere adoptă măsurile de punere în aplicare menționate la articolul xx alineatul (3) din Regulamentul (UE) nr. xxx/2018. Consiliul de conducere poate adopta măsuri suplimentare necesare pentru aplicarea de către Centrul de competențe a Regulamentului (UE) nr. xxx/2018.

Articolul 44

Sprijin din partea statului membru gazdă

Centrul de competențe și statul membru [Belgia] în care se află sediul acestuia pot încheia un acord administrativ referitor la privilegii și imunități, precum și la alte tipuri de sprijin care urmează să fie oferite de statul membru respectiv Centrului de competențe.

CAPITOLUL VII

DISPOZIȚII FINALE

Articolul 45

Acțiuni inițiale

1. Comisiei îi revine răspunderea pentru înființarea și asigurarea exploatării Centrului de competențe în etapa inițială, până când acesta are capacitatea operațională necesară execuției propriului buget. Comisia adoptă, în conformitate cu dreptul Uniunii, toate măsurile necesare cu implicarea organismelor competente ale Centrului de competențe.
2. În sensul alineatului (1), până la preluarea de către directorul executiv a responsabilităților sale în urma numirii sale de către consiliul de conducere, în conformitate cu articolul 16, Comisia poate să desemneze un director executiv interimar și să îndeplinească sarcinile atribuite directorului executiv, care poate fi asistat de un număr limitat de funcționari ai Comisiei. Comisia poate desemna un număr limitat de funcționari proprii, cu titlu provizoriu.
3. După aprobarea prealabilă a consiliului de conducere, directorul executiv interimar poate autoriza toate plățile acoperite de creditele prevăzute în bugetul anual al Centrului de competențe și poate adopta decizii, încheia acorduri și contracte, inclusiv contracte de angajare a personalului, ca urmare a adoptării schemei de personal a Centrului de competențe.
4. Directorul executiv interimar stabilește, de comun acord cu directorul executiv al Centrului de competențe și sub rezerva aprobării de către consiliul de conducere, data la care Centrul de competențe are capacitatea de a-și executa propriul buget. De la data respectivă, Comisia se abține să angajeze credite și să efectueze plăți pentru activitățile Centrului de competențe.

Articolul 46

Durată

1. Centrul de competențe se înființează pentru perioada cuprinsă între 1 ianuarie 2021 și 31 decembrie 2029.
2. La sfârșitul acestei perioade, cu excepția cazului în care se decide altfel prin revizuirea prezentului regulament, se declanșează procedura de lichidare. Procedura de lichidare se declanșează automat în cazul în care Uniunea sau toate statele membre participante se retrag din Centrul de competențe.

3. În scopul derulării procedurilor de lichidare a Centrului de competențe, consiliul de conducere numește unul sau mai mulți lichidatori care se conformează deciziilor consiliului de conducere.

4. În momentul lichidării Centrului de competențe, activele sale sunt utilizate pentru compensarea pasivelor și a cheltuielilor legate de lichidarea sa. Orice surplus se distribuie între Uniune și statele membre participante, proporțional cu contribuția lor financiară la Centrul de competențe. Orice astfel de surplus distribuit Uniunii se restituie bugetului Uniunii.

Articolul 47

Intrare în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președintele	*Președintele*

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

1.2. Domeniul (domeniile) de politică vizat(e) în structura ABM/ABB

1.3. Tipul propunerii/inițiativei

1.4. Obiectiv(e)

1.5. Motivele propunerii/inițiativei

1.6. Durata și impactul financiar

1.7. Modul (modurile) de gestiune preconizat(e)

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

2.2. Sistemul de gestiune și de control

2.3. Măsuri de prevenire a fraudelor și a neregulilor

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

3.2.2. Impactul estimat asupra creditelor operaționale

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ

3.2.4. Compatibilitatea cu cadru financiar multianual actual

3.2.5. Contribuțiile terților

3.3. Impactul estimat asupra veniturilor

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

Regulamentul de instituire a Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică

1.2. Domeniul (domeniile) de politică vizat(e) în structura ABM/ABB[35]

Cercetare și inovare

Investiții strategice europene

1.3. Tipul propunerii/inițiativei

☒Propunerea/inițiativa se referă la **o acțiune nouă**

☐ Propunerea/inițiativa se referă la **o acțiune nouă întreprinsă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[36]

☐ Propunerea/inițiativa se referă la **prelungirea unei acțiuni existente**

☐ Propunerea/inițiativa se referă la **o acțiune reorientată către o acțiune nouă**

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) strategic(e) multianual(e) al(e) Comisiei vizat(e) de propunere/inițiativă

1. O piață unică digitală conectată

2. Un nou impuls pentru locuri de muncă, creștere și investiții

1.4.2. Obiectiv(e) specific(e) vizat(e)

Obiective specifice

1.3 Economia digitală se poate dezvolta la întregul său potențial pe baza unor inițiative care permit dezvoltarea deplină a tehnologiilor digitale și de date.

2.1 Europa își menține poziția de lider mondial în economia digitală, unde întreprinderile europene se pot dezvolta global, bazându-se pe un spirit antreprenorial solid și pe întreprinderi nou înființate performante și unde industria și serviciile publice stăpânesc transformarea digitală.

2.2. Cercetarea europeană identifică oportunități de investiții pentru inovațiile tehnologice potențiale și pentru inițiativele emblematice, în special programul Orizont 2020/Orizont Europa, utilizând parteneriatele public-privat.

---

35 ABM (*activity based management*): gestiune pe activități; ABB (*activity based budgeting*): întocmirea bugetului pe activități.

36 Astfel cum se menționează la articolul 54 alineatul (2) litera (a) sau litera (b) din Regulamentul financiar.

1.4.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care propunerea/inițiativa ar trebui să le aibă asupra beneficiarilor vizați/grupurilor vizate.

Centrul de competențe, împreună cu rețeaua și cu comunitatea, va urmări atingerea următoarelor obiective:

(1) contribuția la punerea în aplicare a părții referitoare la securitatea cibernetică din programul Europa digitală, instituit prin Regulamentul nr. XXX și, în special, a acțiunilor legate de articolul 6 din Regulamentul (UE) nr. XXX [programul Europa digitală], și din programul Orizont Europa, instituit prin Regulamentul nr. XXX și, în special, a secțiunii 2.2.6 din anexa I la Decizia nr. XXX de instituire a programului specific de punere în aplicare a programului-cadru pentru cercetare și inovare Orizont Europa, precum și din alte programe ale Uniunii, atunci când acest lucru este prevăzut în actele juridice ale Uniunii;

(2) consolidarea capacităților, a cunoștințelor și a infrastructurilor în materie de securitate cibernetică în slujba sectoarelor industriale, a sectorului public și a comunităților de cercetare;

(3) contribuția la dezvoltarea pe scară largă a produselor și soluțiilor de securitate cibernetică de ultimă generație în întreaga economie;

(4) îmbunătățirea înțelegerii securității cibernetice și contribuirea la reducerea lacunelor în materie de competențe din Uniune în ceea ce privește securitatea cibernetică;

(5) contribuția la consolidarea cercetării și dezvoltării în domeniul securității cibernetice în Uniune;

(6) consolidarea colaborării dintre domeniile civil și de apărare în ceea ce privește tehnologiile și aplicațiile cu dublă utilizare;

(7) sporirea sinergiilor dintre dimensiunile civilă și de apărare ale securității cibernetice;

(8) facilitarea și contribuția la coordonarea activității Rețelei de centre naționale de coordonare (denumită în continuare „rețeaua”) menționată la articolul 10 și a Comunității de competențe în materie de securitate cibernetică menționate la articolul 12.

1.4.4. Indicatori de rezultat și de impact

A se preciza indicatorii care permit monitorizarea punerii în aplicare a propunerii/inițiativei.

. Numărul de infrastructuri/instrumente de securitate cibernetică achiziționate în comun.

Pentru cercetătorii europeni și industria de profil, oferirea accesului la perioade de testare și experimentare în întreaga rețea și în cadrul centrului. Dacă infrastructurile respective există deja, punerea la dispoziție a unui număr mai mare de ore pentru aceste comunități în comparație cu numărul de ore care le sunt puse la dispoziție în prezent.

. Numărul de comunități ale utilizatorilor deservite și numărul de cercetători care dobândesc acces la infrastructurile europene de securitate cibernetică crește în comparație cu numărul celor care trebuie să caute astfel de resurse în afara Europei.

. Competitivitatea furnizorilor europeni, măsurată în funcție de cota din piața globală (ținta este o cotă de 25% din piață până în 2027), precum și în funcție de procentul de rezultate europene în domeniul cercetării și dezvoltării preluate de industrie, începe să crească.

. Contribuția la următoarele tehnologii de securitate cibernetică, evaluate în funcție de drepturile de autor, brevetele, publicațiile științifice și produsele comerciale.

. Numărul programelor de competențe în materie de securitate cibernetică evaluate și aliniate, numărul programelor de certificare profesională de securitate cibernetică evaluate.

. Numărul de oameni de știință, studenți, utilizatori (din administrația publică și din industrie) care au fost formați.

1.5. Motivele propunerii/inițiativei

1.5.1. Cerință (cerințe) de îndeplinit pe termen scurt sau lung

Atingerea unei mase critice de investiții în dezvoltarea tehnologică și industrială în materie de securitatea cibernetică și depășirea fragmentării capacităților relevante dispersate pe teritoriul UE.

1.5.2. Valoarea adăugată a intervenției UE

Securitatea cibernetică este o problemă de interes comun pentru Uniune, astfel cum au confirmat concluziile Consiliului menționate anterior. Amploarea și caracterul transfrontalier al unor incidente precum WannaCry sau NonPetya constituie un argument în acest sens. Având în vedere natura și amploarea provocărilor tehnologice de securitate cibernetică, precum și coordonarea insuficientă a eforturilor în cadrul industriei, al sectorului public și al comunităților de cercetare, precum și între acestea, UE trebuie să sprijine în continuare eforturile de coordonare, atât pentru a pune în comun o masă critică de resurse, cât și pentru a asigura o mai bună gestionare a cunoștințelor și a activelor. Acest lucru este necesar având în vedere nevoia de resurse legate de anumite capacități de cercetare, dezvoltare și implementare în materie de securitate cibernetică, necesitatea de a oferi acces la know-how interdisciplinar în materie de securitate cibernetică la nivelul diferitelor discipline (adesea doar parțial disponibile la nivel național), natura globală a lanțurilor valorice industriale, precum și activitatea concurenților mondiali activi pe piețe.

Acest lucru necesită resurse și expertiză la un nivel pe care acțiunea individuală a oricărui stat membru nu îl poate atinge într-o măsură suficientă. De exemplu, o rețea paneuropeană de comunicații cuantice ar putea necesita investiții UE de ordinul a 900 de milioane EUR, în funcție de investițiile realizate de statele membre (care urmează să fie interconectate/completate) și de măsura în care tehnologia va permite reutilizarea infrastructurilor existente.

1.5.3. Învățăminte desprinse din experiențe anterioare similare

Evaluarea intermediară a programului Orizont 2020 a confirmat, printre altele, relevanța în continuare a sprijinului UE pentru cercetare și dezvoltare și provocările societale (printre care pachetul financiar aferent clusterului „societăți sigure”, din care este sprijinită cercetarea și dezvoltarea în materie de securitate cibernetică). În același timp, evaluarea confirmă faptul că, în continuare, consolidarea poziției de

lider în sectorul industrial constituie o provocare și că există un decalaj în materie de inovare, UE rămânând în urmă în ceea ce privește inovarea revoluționară creatoare de piețe.

Evaluarea la jumătatea perioadei a Mecanismului pentru interconectarea Europei (MIE) pare să confirme valoarea adăugată a intervenției UE dincolo de domeniul cercetării și dezvoltării, deși preocuparea principală (siguranța în funcționare) și logica intervenției în materie de securitate cibernetică în cadrul MIE sunt oarecum diferite. În același timp, majoritatea beneficiarilor de granturi în materie de securitate cibernetică din cadrul MIE – comunitatea CSIRT-urilor naționale – și-au exprimat dorința de a beneficia de un program de sprijin personalizat în cadrul următorului MIE.

Crearea, în 2016, a parteneriatului public-privat privind securitatea cibernetică în UE a reprezentat un prim pas important prin care comunitățile din cercetare, industrie și sectorul public își unesc eforturile și resursele pentru a facilita cercetarea și inovarea în materie de securitate cibernetică și, în limitele cadrului financiar 2014-2020, acest parteneriat ar trebui să conducă la rezultate bune și mai specifice în domeniul cercetării și inovării. Parteneriatul public-privat a permis partenerilor industriali să-și exprime angajamentul cu privire la cheltuielile individuale în domeniile stabilite în agenda strategică de cercetare și inovare a parteneriatului.

1.5.4. Compatibilitatea și posibila sinergie cu alte instrumente corespunzătoare

Rețeaua de competențe în materie de securitate cibernetică și Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică vor acționa ca un sprijin suplimentar pentru dispozițiile și actorii existenți din domeniul politicii de securitate cibernetică. Mandatul Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică va fi complementar cu eforturile ENISA, însă are o orientare diferită și necesită un set diferit de competențe. În timp ce ENISA își are rolul său de consiliere în ceea ce privește cercetarea și inovarea în materie de securitate cibernetică în UE, mandatul propus se concentrează în primul rând și în cea mai mare măsură asupra altor sarcini esențiale pentru consolidarea rezilienței în materie de securitate cibernetică în UE. Centrul ar trebui să stimuleze dezvoltarea și implementarea tehnologiei în domeniul securității cibernetice și să completeze eforturile de consolidare a capacităților în acest domeniu la nivelul UE și la nivel național.

Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, împreună cu rețeaua de competențe în materie de securitate cibernetică, va acționa, de asemenea, în vederea sprijinirii cercetării pentru facilitarea și accelerarea proceselor de standardizare și de certificare, în special a celor legate de sistemele de certificare de securitate cibernetică în sensul Legii privind securitatea cibernetică.

Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică va acționa ca un organism unic de punere în aplicare pentru două programe ale Uniunii care sprijină securitatea cibernetică (programul Europa digitală și programul Orizont Europa) și va consolida coerența și sinergiile dintre acestea.

Prezenta inițiativă permite completarea eforturilor statelor membre, prin asigurarea unor contribuții adecvate pentru factorii de decizie din domeniul educației în vederea îmbunătățirii educației în materie de securitate cibernetică (de exemplu, prin

dezvoltarea unor programe de învățământ în domeniul securității cibernetice în sistemele educaționale civile și militare, dar și prin contribuții la educația de bază în materie de securitate cibernetică). Inițiativa ar permite, de asemenea, sprijinirea alinierii și a evaluării continue a programelor de certificare de securitate cibernetică profesionale - toate acestea fiind activități necesare pentru a contribui la eliminarea lacunelor în materie de competențe în materie de securitate cibernetică și la facilitarea accesului industriei și al altor comunități la specialiști din domeniul securității cibernetice. Alinierea educației și a competențelor va contribui la dezvoltarea unei forțe de muncă calificate în materie de securitate cibernetică în UE – un atu esențial pentru societățile din domeniul securității cibernetice, precum și pentru alte sectoare interesate de securitatea cibernetică.

1.6. Durata și impactul financiar

☒ Propunere/inițiativă pe **durată determinată**

– ☒ Propunere/inițiativă în vigoare de la 1.1.2021 până la 31.12.2029

– ☒ Impact financiar din 2021 până în 2027 pentru creditele de angajament și din 2021 până în 2031 pentru creditele de plată.

☐ Propunere/inițiativă pe **durată nedeterminată**

– punere în aplicare cu o perioadă de creștere în intensitate din AAAA până în AAAA,

– urmată de o perioadă de funcționare în regim de croazieră.

1.7. Modul (modurile) de gestiune preconizat(e)[37]

☐ **Gestiune directă** asigurată de către Comisie

– ☐ de către serviciile sale, inclusiv prin intermediul personalului din delegațiile Uniunii;

– ☐ de către agențiile executive;

☐ **Gestiune partajată** cu statele membre

☒

Gestiune indirectă cu delegarea sarcinilor de execuție bugetară:

– ☐ țărilor terțe sau organismelor pe care le-au desemnat acestea;

– ☐ organizațiilor internaționale și agențiilor acestora (a se preciza);

– ☐BEI și Fondului european de investiții;

– ☒ organismelor menționate la articolele 70 și 71 din Regulamentul financiar;

– ☐ organismelor de drept public;

– ☐ organismelor de drept privat cu misiune de serviciu public, cu condiția să prezinte garanții financiare adecvate;

– ☐ organismelor de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și care prezintă garanții financiare adecvate;

– ☐ persoanelor cărora li se încredințează executarea unor acțiuni specifice în cadrul PESC, în temeiul titlului V din TUE, identificate în actul de bază relevant.

– *Dacă se indică mai multe moduri de gestiune, a se furniza detalii suplimentare în secțiunea „Observații".*

[37] Explicațiile privind modurile de gestiune, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

A se preciza frecvența și condițiile aferente acestor dispoziții.

Articolul 28 conține dispoziții detaliate privind monitorizarea și raportarea.

2.2. Sistemul de gestiune și de control

2.2.1. Riscul (riscurile) identificat(e)

Pentru a se reduce riscurile legate de funcționarea Centrului de competențe după înființare și eventualele întârzieri, Comisia va sprijini Centrul de competențe în această etapă pentru a asigura recrutarea rapidă a personalului-cheie și instituirea unui sistem eficient de control intern și a unor proceduri solide.

2.2.2. Informații privind sistemul de control intern instituit.

Directorul executiv este responsabil de operațiuni și de gestionarea curentă a Centrului de competențe și este reprezentantul legal al acestuia. Directorul răspunde în fața consiliului de conducere și îi transmite rapoarte în mod continuu cu privire la evoluția activităților Centrului de competențe.

Consiliul de conducere exercită responsabilitatea generală pentru orientarea strategică și operațiunile Centrului de competențe și supraveghează punerea în aplicare a activităților acestuia.

Normele financiare aplicabile centrului de competențe se adoptă de consiliul de conducere după consultarea Comisiei. Acestea nu se abat de la Regulamentul (UE) nr. 1271/2013, cu excepția cazului în care funcționarea Centrului de competențe necesită în mod expres o astfel de abatere, iar Comisia și-a dat acordul prealabil.

Auditorul intern al Comisiei exercită în cazul Centrului de competențe aceleași competențe pe care le exercită în raport cu Comisia. Curtea de Conturi are competența de a-i audita, pe bază de documente și la fața locului, pe toți beneficiarii de granturi, contractanții și subcontractanții care au primit fonduri ale Uniunii din partea Centrului de competențe.

2.2.3. Estimarea costurilor și a beneficiilor controalelor și evaluarea nivelului prevăzut de risc de eroare.

Costul și beneficiile controalelor

Costul controalelor pentru Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică se împarte între costul supravegherii la nivelul Comisiei și costul controalelor operaționale la nivelul organismelor de punere în aplicare.

Costul controalelor la nivelul Centrului de competență este estimat la aproximativ 1,19 % din creditele operaționale de plată executate la nivelul acestuia.

Costul supravegherii la nivelul Comisiei este estimat la aproximativ 1,20 % din creditele operaționale de plată executate la nivelul Centrului de competențe.

Presupunând că activitățile ar fi gestionate în întregime de către Comisie fără sprijinul organismului de punere în aplicare, costul controalelor ar fi substanțial mai mare și ar putea fi de aproximativ 7,7 % din creditele de plată.

Controalele prevăzute au ca scop garantarea unei verificări armonioase și eficiente a entităților de punere în aplicare de către Comisie și a gradului necesar de asigurare la nivelul Comisiei.

Beneficiile controalelor sunt următoarele:

- evitarea selectării unor propuneri mai puțin adecvate sau inadecvate;
- optimizarea planificării și a utilizării fondurilor UE, astfel încât să se mențină valoarea adăugată a UE;
- asigurarea calității acordurilor de grant, pentru a se evita erorile de identificare a entităților juridice, a se asigura calcularea corectă a contribuțiilor UE și a se ține seama de garanțiile necesare pentru o funcționare corectă a granturilor;
- detectarea costurilor neeligibile în etapa de plată;
- detectarea erorilor care afectează legalitatea și regularitatea operațiunilor în etapa de audit.

Nivelul de eroare estimat

Obiectivul este acela de a menține rata erorilor reziduale sub pragul de 2 % pentru întregul program, limitându-se, în același timp, sarcina de control pentru beneficiari, pentru a se realiza un echilibru just între obiectivul legalității și regularității și alte obiective, cum ar fi atractivitatea programului, în special pentru IMM-uri, și costul controalelor.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate.

OLAF poate efectua investigații, inclusiv controale și inspecții la fața locului, în conformitate cu dispozițiile și procedurile prevăzute în Regulamentul 883/2013 al Parlamentului European și al Consiliului și în Regulamentul (Euratom, CE) nr. 2185/9640 al Consiliului din 11 noiembrie 1996 privind controalele și inspecțiile la fața locului efectuate de Comisie în scopul protejării intereselor financiare ale Uniunii împotriva fraudei și a altor abateri, în scopul de a stabili existența unei fraude, a unui act de corupție sau dacă a avut loc orice altă activitate ilegală care afectează interesele financiare ale Uniunii în legătură cu un grant sau un contract finanțat de Centrul de competențe.

Acordurile, deciziile și contractele care rezultă din punerea în aplicare a prezentului regulament trebuie să conțină dispoziții care împuternicesc în mod expres Comisia, Centrul de competențe, Curtea de Conturi și OLAF să efectueze audituri și investigații în conformitate cu competențele lor.

Centrul de competențe se asigură că interesele financiare ale membrilor săi sunt protejate în mod corespunzător prin realizarea sau delegarea realizării unor controale interne și externe adecvate.

Centrul de competențe aderă la Acordul interinstituțional din 25 mai 1999 dintre Parlamentul European, Consiliul Uniunii Europene și Comisia Comunităților Europene privind investigațiile interne efectuate de Oficiul European de Luptă

Antifraudă (OLAF). Centrul de competențe adoptă măsurile necesare pentru facilitarea investigațiilor interne desfășurate de OLAF.

Centrul de competențe va adopta o strategie antifraudă, bazată pe o analiză a riscurilor de fraudă și pe considerente legate de analiza costuri-beneficii. Acesta protejează interesele financiare ale Uniunii prin aplicarea de măsuri preventive de combatere a fraudei, a corupției și a altor activități ilegale, prin realizarea de controale eficace și, dacă se constată nereguli, prin recuperarea sumelor plătite nejustificat și, dacă este cazul, prin sancțiuni administrative și financiare eficace, proporționale și disuasive.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli propusă (propuse)

- Noile linii bugetare solicitate

  În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare:

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul cheltuielilor	Contribuție			
	Număr	Dif./Nedif. [38]	Țări AELS [39]	Țări candidate [40]	Țări terțe	În sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
Rubrica 1: Piața unică, inovare și sectorul digital	01 02 XX XX Orizont Europa, Centrul de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică – cheltuieli de sprijin 01 02 XX XX Orizont Europa, Centrul de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică 02 06 01 XX Programul Europa Digitală, Centrul de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică – cheltuieli de sprijin 02 06 01 XX Programul Europa Digitală, Centrul de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică	Dif.	DA	DA (în cazul în care este specificat în programul anual de lucru)	DA (limitată la anumite părți ale programului)	NU

[38] Dif. = credite diferențiate / Nedif. = credite nediferențiate

[39] AELS: Asociația Europeană a Liberului Schimb.

[40] Țările candidate și, după caz, țările potențial candidate din Balcanii de Vest.

- Se preconizează că pentru aceste linii bugetare contribuțiile vor fi acoperite de:

milioane EUR (cu trei zecimale)

Linia bugetară	Anul 2021	Anul 2022	Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	**Total**
01 01 01 01 Cheltuieli cu funcționarii și agenții temporari responsabili cu cercetarea – Orizont Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Personal extern care pune în aplicare programe de cercetare – Orizont Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Alte cheltuieli de gestiune pentru cercetare – Orizont Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Provocări globale și competitivitate industrială	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Sprijin administrativ – Programul Europa digitală	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Securitatea cibernetică – Programul Europa digitală	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Cheltuieli totale	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Contribuția din pachetul financiar al clusterului „O societate sigură și favorabilă incluziunii” din cadrul pilonului II „Provocări globale și competitivitate industrială” al programului Orizont Europa (pachetul financiar total este de 2 800 000 000 EUR) menționată la articolul 21 alineatul (1) litera (b) va fi propusă de Comisie în cursul procesului legislativ și, în orice caz, înainte de a se ajunge la un acord politic. Propunerea se va baza pe rezultatele procesului de planificare strategică, astfel cum este definit la articolul 6 alineatul (6) din Regulamentul XXX [programul-cadru Orizont Europa].

Sumele de mai sus nu includ contribuția statelor membre la costurile operaționale și administrative ale Centrului de competențe, care este proporțională cu contribuția financiară a Uniunii.

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	**1**	Piața unică, inovare și sectorul digital

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***După 2027***	**TOTAL**
Titlul 1 (Cheltuieli cu personalul)	Angajamente = Plăți	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Titlul 2 (Cheltuieli cu infrastructura și de funcționare)	Angajamente = Plăți	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Titlul 3 (Cheltuieli operaționale)	Angajamente	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Plăți	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
TOTAL credite pentru pachetul	Angajamente	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**

[41] Creditele pentru personal sunt luate în considerare numai pentru o jumătate de an în 2021

financiar al programelor[42]	Plăți	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

[42] Totalul creditelor indicate se referă numai la resursele financiare ale UE dedicate securității cibernetice în cadrul programului Europa digitală. Contribuția din pachetul financiar al clusterului „O societate sigură și favorabilă incluziunii” din cadrul pilonului II „Provocări globale și competitivitate industrială” al programului Orizont Europa (pachetul financiar total este de 2 800 000 000 EUR) menționată la articolul 5 alineatul (1) litera (b) va fi propusă de Comisie în cursul procesului legislativ și, în orice caz, înainte de a se ajunge la un acord politic. Propunerea se va baza pe rezultatele procesului de planificare strategică, astfel cum este definit la articolul 6 alineatul (6) din Regulamentul XXX [programul-cadru Orizont Europa].

Rubrica din cadrul financiar multianual	7	„Cheltuieli administrative”

milioane EUR (cu trei zecimale)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***După 2027***	**TOTAL**
Resurse umane		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Alte cheltuieli administrative		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
TOTAL credite în cadrul RUBRICII 7 din cadrul financiar multianual	(Total angajamente = Total plăți)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

milioane EUR (cu trei zecimale)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***După 2027***	**TOTAL**
TOTAL credite la RUBRICILE cadrului financiar multianual	Angajamente	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Plăți	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 ²061,715**	**2 005,637**

3.2.2. Sinteza impactului estimat asupra creditelor cu caracter administrativ

– ☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ

– ☒ Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

Anii	2021	2022	2023	2024	2025	2026	2027	TOTAL
RUBRICA 7 din cadrul financiar multianual								
Resurse umane	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Alte cheltuieli administrative	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Subtotal RUBRICA 7 din cadrul financiar multianual	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**

În afara RUBRICII 7[43] din cadrul financiar multianual								
Resurse umane								
Alte cheltuieli cu caracter administrativ	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Subtotal în afara RUBRICII 7 din cadrul financiar multianual	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**

TOTAL	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

Necesarul de credite în materie de resurse umane și de alte cheltuieli cu caracter administrativ va fi acoperit de creditele DG-ului care sunt deja alocate pentru gestionarea acțiunii și/sau realocate intern în cadrul DG-ului, completate, după caz, cu resursele suplimentare ce ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și în lumina constrângerilor bugetare.

Creditele de mai sus, necesare pentru resursele umane şi alte cheltuieli de natură administrativă în afara rubricii 7, corespund sumelor acoperite de contribuția financiară a Uniunii din programul Europa digitală.

Creditele necesare pentru resursele umane și alte cheltuieli de natură administrativă în afara rubricii 7 vor fi majorate cu sumele acoperite de contribuția financiară a Uniunii din programul Orizont Europa odată ce contribuția din pachetul financiar al clusterului „O societate sigură și favorabilă incluziunii” din cadrul pilonului II „Provocări globale și competitivitate industrială” al programului Orizont Europa (pachetul financiar total este de 2 800 000 000 EUR) menționată la articolul 21 alineatul (1) litera (b) va fi propusă de Comisie în cursul procesului legislativ și, în orice caz, înainte de a se ajunge la un acord politic.

[43] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

Sumele menționate mai sus ale creditelor necesare pentru resursele umane și alte cheltuieli de natură administrativă în afara rubricii 7 nu includ contribuția statelor membre la costurile administrative ale Centrului de competențe, care este proporțională cu contribuția financiară a Uniunii.

3.2.2.1. Necesarul estimat de resurse umane în Comisie

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

– ■ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimări în echivalent normă întreagă

Anii		2021	2022	2023	2024	2025	2026	2027
• Posturi din schema de personal (funcționari și agenți temporari)								
La sediu și în birourile reprezentanțelor Comisiei		20	21	21	21	21	21	22
Delegații								
Cercetare								
•Personal extern (în echivalent normă întreagă: ENI) - AC, AL, END, INT și JED [44] Rubrica 7								
Finanțare de la RUBRICA 7 din cadrul financiar multianual	- la sediu	3	3	3	3	3	3	3
	- în delegații							
Finanțare din pachetul financiar al programului [45]	- la sediu							
	- în delegații							
Cercetare								
Altele (precizați)								
TOTAL		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau realocate intern în cadrul DG-ului, completate, după caz, cu resursele suplimentare ce ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii de alocare anuală și în lumina constrângerilor bugetare.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și agenți temporari	Coordonarea, monitorizarea și îndrumarea sarcinilor încredințate Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, inclusiv costurile de sprijin și de coordonare. Elaborarea de politici și coordonarea în domeniul securității cibernetice în ceea ce privește sarcinile încredințate Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, de exemplu, în ceea ce privește stabilirea priorităților pentru politica de cercetare și industrială, cooperarea generală dintre statele membre și operatorii economici, coerența cu viitorul cadru UE de certificare de securitate cibernetică, activitatea privind răspunderea și obligația de diligență sau coordonarea cu politicile privind HPC, IA și competențele digitale. .
Personal extern	Coordonarea, monitorizarea și îndrumarea sarcinilor încredințate Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, inclusiv costurile de sprijin și de coordonare. Elaborarea de politici și coordonarea în domeniul securității cibernetice în ceea ce privește sarcinile încredințate Centrului de competențe european industrial, tehnologic și

[44] AC = agent contractual; AL = agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JED = expert tânăr în delegații.

[45] Subplafonul pentru personal extern acoperit din creditele operaționale (fostele linii „BA”).

	de cercetare în materie de securitate cibernetică, de exemplu, în ceea ce privește stabilirea priorităților pentru politica de cercetare și industrială, cooperarea generală dintre statele membre și operatorii economici, coerența cu viitorul cadru UE de certificare de securitate cibernetică, activitatea privind răspunderea și obligația de diligență sau coordonarea cu politicile privind HPC, IA și competențele digitale. .

3.2.2.2. Necesarul estimat de resurse umane din cadrul Centrului de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică

	2021	2022	2023	2024	2025	2026	2027
Funcționari ai Comisiei							
din care AD							
din care AST							
din care AST-SC							
Agenți temporari							
din care AD	10	11	13	13	13	13	13
din care AST							
din care AST-SC							
Agenți contractuali	26	32	39	39	39	39	39
Experți naționali detașați	1	1	1	1	1	1	1
Total	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Descrierea sarcinilor care trebuie efectuate:

Funcționari și agenți temporari	Punerea în aplicare operațională a sarcinilor încredințate Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică în temeiul articolului 4 din prezentul regulament, inclusiv costurile de sprijin și de coordonare.
Personal extern	Punerea în aplicare operațională a sarcinilor încredințate Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică în temeiul articolului 4 din prezentul regulament, inclusiv costurile de sprijin și de coordonare.

Necesarul de resurse umane estimat mai sus, din cadrul Centrului de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică corespunde cerințelor estimate pentru execuția contribuției financiare a Uniunii din cadrul programului Europa digitală.

Necesarul de resurse umane estimat mai sus, din cadrul Centrului de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică va fi mărit cu necesarul estimat pentru execuția contribuției financiare a Uniunii din cadrul programului Orizont Europa odată ce contribuția din pachetul financiar al clusterului „O societate sigură și favorabilă incluziunii” din cadrul pilonului II „Provocări globale și competitivitate industrială” al programului Orizont Europa (pachetul financiar total este de 2 800 000 000 EUR) menționată la articolul 21 alineatul (1) litera (b) va fi propusă de Comisie în cursul procesului legislativ și, în orice caz, înainte de a se ajunge la un acord politic.

3.2.2.3. Schema de personal a Centrului de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică

Grupa de funcții și gradul	2021	2022	2023	2024	2025	2025	2025
AD 16							

AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
AD Total	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
AST Total							
AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							

AST/SC 2							
AST/SC 1							
AST/SC Total							
TOTAL GENERAL	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Impactul estimat asupra personalului (suplimentar) — personalul extern al Centrului de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică

Agenți contractuali	2021	2022	2023	2024	2025	2026	2027
Grupa de funcții IV	20	22	29	29	29	29	29
Grupa de funcții III	2	4	4	4	4	4	4
Grupa de funcții II	4	6	6	6	6	6	6
Grupa de funcții I							
Total	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Pentru a asigura neutralitatea în ceea ce privește numărul de angajați, efectivele de personal suplimentar din Centrul de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică vor fi parțial compensate prin reducerea numărului de funcționari și de personal extern (și anume, schema de personal și personalul extern existent) din cadrul serviciilor relevante ale Comisiei.

Efectivele de personal din Centrul de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică de la punctele 3.2.2.2-4 vor fi compensate după cum urmează[46]:

TOTAL	2021	2022	2023	2024	2025	2026	2027
Funcționari ai Comisiei	5	5	6	6	6	6	6
Agenți temporari							
Agenți contractuali	14	17	20	20	20	20	20
Experți naționali detașați							
Total ENI	19	22	26	26	26	26	26
Angajați	19	22	26	26	26	26	26

[46] Sub rezerva sumei finale a bugetului a cărui execuție va fi delegată Centrului de competențe

Compensarea resurselor umane din cadrul Centrului de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică va fi proporțională cu contribuția financiară a Uniunii, și anume 50%.

Compensarea de mai sus este legată de necesarul estimat mai sus de resurse umane din cadrul Centrului de competențe industrial, tehnologic și de cercetare în materie de securitate cibernetică pentru punerea în aplicare a contribuției financiare a Uniunii din cadrul programului Europa digitală.

Compensarea de mai sus va fi majorată cu necesarul estimat pentru punerea în aplicare a contribuției financiare a Uniunii de la programul Orizont Europa odată ce contribuția din pachetul financiar al clusterului „O societate sigură și favorabilă incluziunii” din cadrul pilonului II „Provocări globale și competitivitatea industrială” al programului Orizont Europa (pachetul financiar total este de 2 800 000 000 EUR) menționată la articolul 21 alineatul (1) litera (b) va fi propusă de Comisie în cursul procesului legislativ și, în orice caz, înainte de a se ajunge la un acord politic.

3.2.3. Contribuția terților

Propunerea/inițiativa:

– ☐ nu prevede cofinanțare din partea terților

– ☒ prevede cofinanțare din partea terților[47], estimată în cele ce urmează:

Credite în milioane EUR (cu trei zecimale)

Anii	2021	2022	2023	2024	2025	2026	2027	TOTAL
Statele membre – contribuția la cheltuielile cu personalul	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Statele membre – contribuția la cheltuielile cu infrastructura și de funcționare	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Statele membre – contribuția la cheltuielile operaționale	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
TOTAL credite cofinanțate	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Contribuția terților menționată mai sus se referă numai la cofinanțarea proporțională cu resursele financiare ale UE dedicate securității cibernetice în cadrul programului Europa digitală. Contribuția terților menționată mai sus va fi majorată odată ce contribuția financiară din clusterul „O societate sigură și favorabilă incluziunii” din cadrul pilonului II „Provocări globale și competitivitate industrială” al programului Orizont Europa (pachetul financiar total este de 2 800 000 000 EUR) menționată la articolul 21 alineatul (1) litera (b) va fi propusă de Comisie în cursul procesului legislativ și, în orice caz, înainte de a se ajunge la un acord politic. Propunerea se va baza pe rezultatele procesului de planificare strategică, astfel cum este definit la articolul 6 alineatul (6) din Regulamentul XXX [programul-cadru Orizont Europa].

3.3. Impactul estimat asupra veniturilor

– ☒ Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☐ Propunerea/inițiativa are următorul impact financiar:

☐ asupra resurselor proprii

☐ asupra altor venituri

vă rugăm să precizați dacă veniturile sunt alocate unor linii de cheltuieli ☐

milioane EUR (cu trei zecimale)

Linia bugetară pentru	Impactul propunerii/inițiativei[48]

[47] Contribuții în natură estimate din partea statelor membre

[48] În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sume brute după deducerea unei cote de 20 % pentru costuri de colectare.

venituri:	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Articolul …….							

Pentru veniturile alocate, a se preciza linia bugetară (liniile bugetare) de cheltuieli afectată (afectate).

Alte observații (de exemplu, metoda/formula utilizată pentru calcularea impactului asupra veniturilor sau orice alte informații).