COMMISSIONE
EUROPEA

Bruxelles, 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento

Contributo della Commissione europea per la riunione dei leader del 19-20 settembre 2018 a Salisburgo

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

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

Vista la crescente dipendenza della vita quotidiana e delle economie dalle tecnologie digitali, i cittadini sono sempre più esposti a gravi incidenti informatici. La sicurezza futura dipende dal potenziamento della capacità di proteggere l'Unione europea dalle minacce informatiche, in quanto sia le infrastrutture civili che le capacità militari devono poter fare affidamento su sistemi digitali sicuri.

Per far fronte alle sfide crescenti, l'Unione ha costantemente intensificato le sue attività nel settore, basandosi sulla strategia per la cibersicurezza del 2013[1] e sui suoi obiettivi e principi per promuovere un ecosistema cibernetico affidabile, sicuro e aperto. Nel 2016 l'Unione ha adottato le sue prime misure nel settore della cibersicurezza attraverso la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio[2] sulla sicurezza delle reti e dei sistemi informativi.

Alla luce della rapida evoluzione del panorama della cibersicurezza, nel settembre 2017 la Commissione e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato la comunicazione congiunta[3] "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE" per rafforzare ulteriormente la resilienza, la deterrenza e la risposta dell'Unione agli attacchi informatici. Nella comunicazione congiunta, che trae fondamento anche da iniziative precedenti, viene proposta una serie di azioni comprendenti, tra l'altro, il consolidamento dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), la creazione di un quadro volontario di certificazione della cibersicurezza a livello dell'UE per aumentare la sicurezza informatica dei prodotti e dei servizi nel mondo digitale e un piano per una risposta rapida e coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.

Nella comunicazione congiunta è stato rilevato che è anche nell'interesse strategico dell'UE garantire il mantenimento e lo sviluppo di capacità tecnologiche essenziali in materia di sicurezza informatica per tutelare il proprio mercato unico digitale e, in particolare, per proteggere reti e sistemi informativi critici e fornire servizi fondamentali di cibersicurezza. L'Unione deve essere in grado di salvaguardare le proprie risorse digitali e competere sul mercato mondiale della cibersicurezza.

Al momento, l'Unione è un importatore netto di prodotti e soluzioni in questo settore e dipende fortemente da fornitori non europei[4]. Il mercato mondiale della cibersicurezza ha un valore di 600 miliardi di EUR e si prevede che nei prossimi cinque anni crescerà in media del

---

1 COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO: Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro, JOIN(2013) 1 final.

2 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

3 COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO: Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE, JOIN(2017) 450 final.

4 Progetto di relazione finale sullo studio di mercato in materia di cibersicurezza, 2018.

17% circa in termini di vendite, numero di aziende e occupazione. Tuttavia, tra i primi 20 paesi leader nel mercato della sicurezza informatica figurano solo sei Stati membri[5].

Contestualmente, l'Unione vanta grandi competenze ed esperienza nella cibersicurezza, con oltre 660 organizzazioni in tutta l'UE registrate nell'ambito della recente mappatura dei centri di competenza nel settore condotta dalla Commissione[6]. Queste competenze, una volta trasformate in prodotti e soluzioni commercializzabili, potrebbero consentire all'Unione di coprire tutta la catena di valore della cibersicurezza. Tuttavia, gli sforzi delle comunità della ricerca e dell'industria sono frammentati, disallineati e privi di una progettualità comune, il che frena la competitività dell'UE in questo ambito e la sua capacità di tutelare le proprie risorse digitali. Oggi i settori pertinenti in materia di cibersicurezza (per esempio l'energia, lo spazio, la difesa e i trasporti) e i relativi sottosettori non sono sostenuti a sufficienza[7]; non vengono sfruttate appieno neppure le sinergie tra i settori della cibersicurezza civile e della difesa.

La creazione nel 2016 del partenariato pubblico-privato ("cPPP") sulla cibersicurezza nell'Unione ha costituito un importante primo passo, che riunisce le comunità della ricerca, dell'industria e del settore pubblico per agevolare la ricerca e l'innovazione nella sicurezza informatica e che, entro i limiti del quadro finanziario 2014-2020, dovrebbe produrre risultati validi e maggiormente mirati nell'ambito della ricerca e dell'innovazione. Il cPPP ha consentito ai partner industriali di manifestare il loro impegno per quanto riguarda le spese da essi sostenute in aree definite nell'agenda strategica del partenariato per la ricerca e l'innovazione.

Tuttavia, l'Unione può perseguire un investimento su scala molto più vasta e necessita di un meccanismo più efficace per creare capacità durature, mettere in comune sforzi e competenze e stimolare lo sviluppo di soluzioni innovative che rispondano alle sfide industriali della cibersicurezza nel campo delle nuove tecnologie multiuso (per esempio l'intelligenza artificiale, l'informatica quantistica, la blockchain e le identità digitali sicure) e in settori critici (per esempio i trasporti, l'energia, la sanità, le finanze, l'amministrazione, le telecomunicazioni, la produzione, la difesa e lo spazio).

Nella comunicazione congiunta è stata considerata la possibilità di rafforzare la capacità dell'Unione in materia di sicurezza informatica per mezzo di una rete di centri di competenza nel settore della cibersicurezza imperniata su un apposito centro di competenza europeo, nell'intento di integrare gli sforzi attuali di creazione delle capacità in quest'ambito a livello nazionale e di Unione. Nella comunicazione congiunta è stata espressa l'intenzione della Commissione di avviare una valutazione d'impatto nel 2018 per esaminare le opzioni disponibili con l'obiettivo di istituire tale struttura. Come primo passo, per indirizzare il pensiero futuro, la Commissione ha varato una fase pilota nell'ambito di Orizzonte 2020, al fine di contribuire a riunire i centri nazionali in una rete per dare nuovo slancio alle competenze nel campo della cibersicurezza e allo sviluppo tecnologico.

In occasione del vertice di Tallinn sul digitale del settembre 2017, i capi di Stato e di governo hanno invitato l'Unione a diventare "un leader mondiale della cibersicurezza entro il 2025, al fine di garantire la fiducia, la sicurezza e la tutela dei nostri cittadini, dei nostri consumatori e delle nostre imprese online e di fare sì che Internet sia libero e regolamentato".

---

5 Progetto di relazione finale sullo studio di mercato in materia di cibersicurezza, 2018.

6 Relazioni tecniche del CCR: Centri di competenza europei nel settore della cibersicurezza, 2018.

7 Relazione tecnica del CCR: Risultati dell'attività di mappatura (cfr. allegati 4 e 5 per i dettagli).

Le conclusioni del Consiglio[8] adottate nel novembre 2017 hanno sollecitato la Commissione a fornire rapidamente una valutazione d'impatto sulle opzioni possibili e a proporre entro la metà del 2018 lo strumento giuridico pertinente per l'attuazione dell'iniziativa.

Il programma Europa digitale proposto dalla Commissione nel giugno 2018[9] mira ad ampliare e a massimizzare i vantaggi della trasformazione digitale per i cittadini e le imprese europei in tutti i settori strategici pertinenti dell'UE, rafforzando le politiche e sostenendo le ambizioni del mercato unico digitale. Il programma propone un approccio coerente e di vasto respiro per garantire l'impiego ottimale di tecnologie avanzate e la giusta combinazione di capacità tecnica e competenza umana per la trasformazione digitale, non solo nel settore della cibersicurezza, ma anche per quanto riguarda l'infrastruttura di dati intelligente, l'intelligenza artificiale, competenze digitali avanzate e applicazioni nell'industria e nei settori di interesse pubblico. Questi elementi sono interdipendenti, complementari e, quando vengono promossi simultaneamente, possono raggiungere le dimensioni necessarie per rendere prospera l'economia dei dati[10]. Anche *Orizzonte Europa*[11], il prossimo programma quadro di R&I dell'UE, include la cibersicurezza tra le sue priorità.

In tale contesto, con il presente regolamento viene proposta l'istituzione di un Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza con una rete di centri nazionali di coordinamento. Per incentivare l'ambiente tecnologico e industriale europeo che opera nel settore della cibersicurezza, questo modello di cooperazione *ad hoc* dovrebbe funzionare come segue. Il Centro di competenza dovrebbe agevolare e coordinare il lavoro della rete e fungere da riferimento per la comunità delle competenze in materia di cibersicurezza, impostando l'agenda tecnologica in tema di cibersicurezza e facilitando l'accesso alle competenze acquisite. In particolare, il Centro di competenza dovrebbe attuare le parti pertinenti dei programmi Europa digitale e Orizzonte Europa stanziando fondi e occupandosi degli appalti. Visti gli investimenti ingenti in cibersicurezza che sono stati fatti in altre parti del mondo e considerata la necessità di un coordinamento e di una condivisione delle risorse del settore in Europa, viene proposto di configurare il Centro di competenza come partenariato europeo[12], di modo che risultino agevolati gli investimenti congiunti dell'Unione, degli Stati membri e/o dell'industria. La proposta prevede pertanto che gli Stati membri contribuiscano con un importo commisurato alle attività del Centro di competenza e della rete. Il principale organo decisionale sarà il consiglio di direzione, nel quale saranno rappresentati tutti gli Stati membri ma avranno diritto di voto soltanto gli Stati membri che contribuiscono finanziariamente. Il meccanismo di voto del consiglio di direzione seguirà il principio della doppia maggioranza, fissata al 75% del contributo finanziario e al 75% dei voti. In considerazione della sua responsabilità rispetto al bilancio dell'Unione, la Commissione deterrà il 50% dei voti. Per le sue attività inerenti al consiglio di direzione, se

---

8 Conclusioni del Consiglio sulla comunicazione congiunta al Parlamento europeo e al Consiglio: Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE, adottate dal Consiglio "Affari generali" il 20 novembre 2017.

9 COM(2018) 434 Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce il programma Europa digitale per il periodo 2021-2027.

10 Cfr. SWD(2018) 305.

11 COM(2018) 435 Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce Orizzonte Europa - il programma quadro di ricerca e innovazione - e ne stabilisce le norme di partecipazione e diffusione.

12 Come da definizione in COM(2018) 435 Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce Orizzonte Europa - il programma quadro di ricerca e innovazione - e ne stabilisce le norme di partecipazione e diffusione e da riferimento in COM(2018) 434 Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce il programma Europa digitale per il periodo 2021-2027.

del caso la Commissione potrà avvalersi del patrimonio di competenze del Servizio europeo per l'azione esterna. Il Centro di competenza sarà assistito da un consiglio consultivo industriale e scientifico che garantirà il dialogo periodico con il settore privato, le organizzazioni dei consumatori e gli altri soggetti interessati.

Operando a stretto contatto con la rete dei centri nazionali di coordinamento e la comunità delle competenze in materia di cibersicurezza (che coinvolge un gruppo vasto e diversificato di operatori impegnati nello sviluppo tecnologico nell'ambito della cibersicurezza, quali enti di ricerca, industrie sul versante dell'offerta e su quello della domanda, nonché il settore pubblico) istituita dal presente regolamento, il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza costituirebbe l'organo esecutivo principale per le risorse finanziarie dell'UE dedicate alla sicurezza informatica nell'ambito dei programmi proposti, *Europa digitale* e *Orizzonte Europa*.

Un approccio così ampio permetterebbe di promuovere la cibersicurezza attraverso l'intera catena del valore, dalla ricerca al sostegno dell'implementazione e della diffusione di tecnologie chiave. La partecipazione finanziaria degli Stati membri dovrebbe essere commisurata al contributo finanziario per questa iniziativa ed è un elemento indispensabile per il suo successo.

Considerando le sue particolari competenze e l'ampia e significativa rappresentanza dei portatori di interessi, l'Organizzazione europea per la cibersicurezza, che costituisce la controparte della Commissione nel partenariato pubblico-privato contrattuale sulla cibersicurezza nell'ambito di Orizzonte 2020, dovrebbe essere invitata a contribuire all'attività del Centro e della rete.

Inoltre, il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza dovrebbe anche adoperarsi per potenziare le sinergie tra le dimensioni civile e di difesa della sicurezza informatica e sostenere gli Stati membri e altri soggetti pertinenti fornendo consulenza, condividendo competenze e agevolando la collaborazione in merito al progetto e alle azioni. Qualora lo richiedano gli Stati membri, il Centro potrebbe agire in qualità di responsabile del progetto, in particolare per quanto riguarda il Fondo europeo per la difesa. La presente iniziativa mira a contribuire alla soluzione dei seguenti problemi:

- **l'insufficiente cooperazione tra le industrie della cibersicurezza sul versante della domanda e dell'offerta.** Le aziende europee sono alle prese con una duplice sfida: rimanere sicure e offrire al tempo stesso prodotti e servizi sicuri ai loro clienti. Tuttavia, spesso non sono in grado di fornire garanzie adeguate per i loro prodotti, servizi e beni o di progettare prodotti e servizi innovativi sicuri. Per gli operatori privati la cui attività commerciale principale non è connessa alla cibersicurezza, sviluppare e mettere in atto risorse chiave in questo settore risulta troppo costoso. Contestualmente, i rapporti tra il versante della domanda e quello dell'offerta del mercato della cibersicurezza non sono sufficientemente sviluppati, per cui si ha un'offerta non ottimale di soluzioni e prodotti europei adatti alle esigenze dei diversi settori, oltre a livelli di fiducia insufficienti presso gli operatori del mercato;
- **la mancanza di un meccanismo di cooperazione efficace tra Stati membri per la creazione delle capacità industriali.** Al momento non esiste un meccanismo di cooperazione efficace che permetta agli Stati membri di collaborare allo sviluppo delle capacità necessarie a sostegno dell'innovazione della sicurezza informatica nei vari settori industriali e della realizzazione di soluzioni europee di cibersicurezza all'avanguardia. I meccanismi di cooperazione esistenti per gli Stati membri nel campo della sicurezza

informatica contemplati dalla direttiva (UE) 2016/1148 non prevedono questo tipo di attività nel loro mandato;

- **l'insufficiente cooperazione delle comunità della ricerca e dell'industria, tanto al loro interno che fra loro.** Malgrado l'Europa disponga della capacità teorica di coprire l'intera catena di valore della cibersicurezza, in tale ambito ci sono settori (per esempio l'energia, lo spazio, la difesa, i trasporti) e relativi sottosettori che al giorno d'oggi sono scarsamente sostenuti dalla comunità della ricerca o sono sostenuti solo da un limitato numero di centri (per esempio la crittografia post-quantistica e quantistica, la fiducia e la sicurezza informatica nell'intelligenza artificiale). Anche se, ovviamente, questa collaborazione esiste, spesso si tratta di accordi a breve termine, simili consulenze, che non permettono di impostare piani di ricerca nel lungo periodo per superare le sfide industriali della cibersicurezza;
- **l'insufficiente cooperazione tra le comunità della ricerca e dell'innovazione operanti nel settore della cibersicurezza civile e quelle attive nel campo della cibersicurezza per la difesa.** Il problema costituito dal grado insufficiente di cooperazione riguarda anche la comunità civile e quella della difesa. Le sinergie esistenti non vengono utilizzate appieno a causa della mancanza di meccanismi efficaci che consentano a tali comunità di cooperare efficacemente e di instaurare un clima di fiducia che, ancor più che in altri campi, costituisce una *conditio sine qua non* per una cooperazione proficua. A ciò si aggiungono le capacità finanziarie limitate del mercato della cibersicurezza dell'UE, ivi compresa l'insufficienza di fondi per sostenere l'innovazione.
- **Coerenza con le disposizioni vigenti nel settore normativo interessato**

La rete di competenza per la cibersicurezza e il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza apporteranno un ulteriore sostegno alle disposizioni regolamentari e agli operatori del settore della sicurezza informatica. Il mandato del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza integrerà gli sforzi dell'ENISA, ma ha un obiettivo diverso e richiede un insieme di competenze differente. Per quanto l'incarico dell'ENISA preveda un ruolo di consulenza in tema di ricerca e innovazione per la cibersicurezza nell'UE, il mandato proposto per quest'agenzia si concentra innanzitutto su altri compiti cruciali per il rafforzamento della resilienza in materia di cibersicurezza nell'Unione. Inoltre il mandato dell'ENISA non contempla i tipi di attività che costituirebbero le funzioni principali del Centro e della rete, ossia stimolare lo sviluppo e l'implementazione della tecnologia per la cibersicurezza e integrare l'impegno per la creazione di capacità in questo settore a livello dell'UE e nazionale.

Il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza collaborerà con la rete di competenza per la cibersicurezza nel sostenere la ricerca per agevolare e accelerare i processi di standardizzazione e certificazione, in particolare quelli relativi ai sistemi di certificazione della cibersicurezza ai sensi della proposta di regolamento sulla cibersicurezza[13][14].

---

[13] Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza, COM(2017) 477 final/3").

[14] Ciò non pregiudica i meccanismi di certificazione previsti dal regolamento generale sulla protezione dei dati, con il coinvolgimento delle autorità per la protezione dei dati, conformemente al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle

La presente iniziativa amplia *de facto* il partenariato pubblico-privato sulla cibersicurezza (cPPP), che ha rappresentato il primo tentativo a livello di UE di riunire l'industria della cibersicurezza, il versante della domanda (acquirenti di prodotti e soluzioni per la sicurezza informatica, anche nell'ambito della pubblica amministrazione e in settori critici, quali per esempio i trasporti, la sanità, l'energia, le finanze) e la comunità della ricerca per costruire la piattaforma del dialogo sostenibile e creare le condizioni per il coinvestimento volontario. Il cPPP, istituito nel 2016, ha determinato investimenti per 1,8 miliardi di EUR fino al 2020. L'entità dell'investimento in corso in altre parti del mondo (per esempio, gli Stati Uniti hanno investito 19 miliardi di dollari nella cibersicurezza solo nel 2017) indica tuttavia che l'UE deve fare di più per raggiungere una massa critica di investimenti e superare la frammentazione delle capacità nell'Unione.

- **Coerenza con le altre politiche dell'Unione**

Il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza agirà come organo esecutivo unico per vari programmi dell'Unione a sostegno della cibersicurezza (programmi Europa digitale e Orizzonte Europa), aumentando la coerenza e le sinergie tra di essi.

Questa iniziativa permetterà inoltre di integrare gli sforzi degli Stati membri fornendo un contributo adeguato ai responsabili delle politiche dell'istruzione, al fine di potenziare le competenze relative alla cibersicurezza (per esempio mettendo a punto piani formativi sulla materia per i sistemi di istruzione a livello civile e militare) per contribuire allo sviluppo di una forza lavoro qualificata nell'UE nell'ambito della sicurezza informatica, una risorsa fondamentale per le aziende operanti nel campo della cibersicurezza e per le altre industrie interessate. Per quanto concerne l'istruzione e la formazione in materia di ciberdifesa, questa iniziativa è coerente con le attività in corso nell'ambito delle piattaforme dell'istruzione, della formazione e delle esercitazioni istituite nel contesto dell'Accademia europea per la sicurezza e la difesa.

Questa iniziativa integrerà e sosterrà gli sforzi dei poli dell'innovazione digitale nell'ambito del programma Europa digitale. I poli dell'innovazione digitale sono organizzazioni senza fini di lucro che aiutano le aziende (in particolare le start-up, le PMI e le imprese a media capitalizzazione) ad aumentare la loro competitività migliorando i loro processi aziendali/produttivi e i loro prodotti e servizi attraverso l'innovazione intelligente resa possibile dalla tecnologia digitale. I poli dell'innovazione digitale forniscono servizi innovativi orientati alle imprese, come le informazioni sul mercato, la consulenza finanziaria, l'accesso a strutture di prova e sperimentazione, la formazione e lo sviluppo di competenze, per far sì che nuovi prodotti o servizi raggiungano il mercato con successo o per realizzare processi produttivi migliori. Alcuni poli dell'innovazione digitale con competenze specifiche nel settore della cibersicurezza potrebbero essere coinvolti direttamente nella comunità delle competenze in materia di cibersicurezza istituita da questa iniziativa. Nella maggior parte dei casi, tuttavia, i poli dell'innovazione digitale che non possiedono un profilo specifico per quanto concerne la cibersicurezza faciliterebbero l'accesso della loro base di utenti alle competenze, alle conoscenze e alle capacità in materia di sicurezza informatica disponibili presso la suddetta comunità cooperando strettamente con la rete dei centri nazionali di coordinamento e il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza. I poli dell'innovazione digitale promuoverebbero inoltre la diffusione di

---

persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("regolamento generale sulla protezione dei dati").

soluzioni e prodotti innovativi per la sicurezza informatica che rispondano alle esigenze delle aziende e degli altri utenti finali che ne usufruiscono. Da ultimo, ma non meno importante, i poli dell'innovazione digitale specializzati in determinati settori potrebbero condividere le loro conoscenze sulle esigenze settoriali concrete con la rete e il Centro per alimentare la riflessione sull'agenda per la ricerca e l'innovazione, venendo incontro alle esigenze dell'industria.

Si perseguiranno sinergie con le comunità della conoscenza e dell'innovazione pertinenti dell'Istituto europeo di innovazione e tecnologia e, in particolare, con l'IET Digitale.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- **Base giuridica**

Il Centro di competenza dovrebbe fondarsi su una doppia base giuridica per via della sua natura e dei suoi obiettivi specifici. L'articolo 187 del TFUE, in base al quale possono essere istituite le strutture dell'Unione necessarie alla migliore esecuzione dei programmi di ricerca, sviluppo tecnologico e dimostrazione, consente al Centro di competenza di creare sinergie e aggregare risorse per investire in capacità indispensabili a livello degli Stati membri e sviluppare risorse europee comuni (per esempio attraverso l'acquisto congiunto delle necessarie infrastrutture di prova e sperimentazione in materia di cibersicurezza). Il primo comma dell'articolo 188 prevede l'adozione di tali misure; nondimeno, se tale comma costituisse l'unica base giuridica, le attività non potrebbero spingersi al di là della sfera della ricerca e dello sviluppo, come invece è necessario per conseguire tutti gli obiettivi del Centro di competenza stabiliti nel presente regolamento che promuovono la diffusione sul mercato di prodotti e soluzioni per la sicurezza informatica, aiutano l'industria europea della cibersicurezza a diventare maggiormente competitiva, aumentandone la quota di mercato, e creano un valore aggiunto per gli sforzi nazionali volti a superare il divario di competenze in materia di cibersicurezza. Pertanto, al fine di conseguire i suddetti obiettivi, è necessario aggiungere l'articolo 173, paragrafo 3, come base giuridica, per consentire all'Unione di mettere in atto misure a sostegno della competitività dell'industria.

- **Motivazione della proposta alla luce dei principi di proporzionalità e sussidiarietà**

La sicurezza informatica è una questione di interesse comune dell'Unione, come confermano le conclusioni del Consiglio sopra indicate e la portata e il carattere transfrontaliero di incidenti come quelli costituiti da *WannaCry* e *NonPetya*. La natura e l'entità dei problemi tecnologici della cibersicurezza e il coordinamento insufficiente degli sforzi all'interno delle comunità dell'industria, del settore pubblico e della ricerca, nonché fra tali comunità, richiedono un ulteriore sostegno degli sforzi di coordinamento da parte dell'UE sia per aggregare una massa critica di risorse sia per garantire una migliore conoscenza e gestione delle risorse. Ciò è necessario se si considera il fabbisogno di risorse correlato a determinate capacità di ricerca, sviluppo e implementazione della cibersicurezza, l'esigenza di fornire accesso a competenze interdisciplinari in materia di sicurezza informatica nell'ambito di discipline diverse (accesso che sovente è disponibile solo in parte a livello nazionale), la natura globale delle catene di valore industriale, nonché l'attività dei concorrenti a livello mondiale che operano sui vari mercati.

Ciò richiede una quantità di risorse e competenze che difficilmente l'iniziativa individuale di un qualsiasi Stato membro riesce a mobilitare. Per esempio, una rete paneuropea di comunicazioni quantistiche potrebbe richiedere un investimento dell'UE di circa 900 milioni

di EUR, a seconda degli investimenti effettuati dagli Stati membri (da collegare/integrare) e della misura in cui la tecnologia consentirà di riutilizzare le infrastrutture esistenti. L'iniziativa sarà fondamentale per riunire i finanziamenti e permettere di effettuare questo tipo di investimento nell'Unione.

Gli Stati membri non possono conseguire appieno gli obiettivi di questa iniziativa da soli; come indicato sopra, tali obiettivi possono essere meglio conseguiti a livello di Unione unendo gli sforzi ed evitandone l'inutile duplicazione, contribuendo al raggiungimento della massa critica degli investimenti e garantendo un impiego ottimale del finanziamento pubblico. Contestualmente, il presente regolamento si limita a quanto necessario per conseguire tali scopi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo. L'azione dell'UE è pertanto giustificata in termini di sussidiarietà e proporzionalità.

Questo atto giuridico non prevede nuovi obblighi normativi per le imprese. Nel contempo, le imprese e in particolare le PMI potranno probabilmente ridurre le spese correlate ai loro sforzi per la progettazione di prodotti innovativi e sicuri dal punto di vista cibernetico, poiché l'iniziativa consente di aggregare risorse per investire in capacità necessarie a livello di Stati membri o sviluppare risorse europei comuni (per esempio attraverso l'acquisto congiunto delle necessarie infrastrutture di prova e sperimentazione in materia di cibersicurezza). Tali risorse potrebbero essere utilizzate da industrie e PMI di diversi settori per garantire la sicurezza informatica dei loro prodotti e trasformare la cibersicurezza in un loro vantaggio competitivo.

- **Scelta dell'atto giuridico**

L'atto giuridico proposto istituisce un organismo preposto all'attuazione di azioni in materia di cibersicurezza nell'ambito dei programmi Europa digitale e Orizzonte Europa, definendone il mandato, i compiti e la struttura di governance. L'istituzione di un tale organismo dell'Unione richiede l'adozione di un regolamento.

3. CONSULTAZIONE DEI PORTATORI DI INTERESSI E VALUTAZIONI D'IMPATTO

La proposta di creare una rete di competenza per la cibersicurezza con un Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza è una nuova iniziativa, che costituisce un proseguimento e un'evoluzione del partenariato pubblico-privato contrattuale sulla sicurezza istituito nel 2016.

- **Consultazione dei portatori di interessi**

La cibersicurezza è un tema ampio e transettoriale. La Commissione si è servita di diversi metodi di consultazione al fine di garantire che la presente iniziativa tenga debitamente conto dell'interesse pubblico generale dell'Unione, invece che degli interessi specifici di un ambito ristretto di gruppi di portatori di interessi. Questo metodo assicura la trasparenza e la responsabilità dell'operato della Commissione. Benché non siano state effettuate consultazioni pubbliche aperte appositamente per questa iniziativa, dati i suoi destinatari (comunità della ricerca e dell'industria e Stati membri) la tematica è stata già trattata da molte altre consultazioni pubbliche aperte:

- una consultazione pubblica generale aperta, condotta nel 2018 sui temi degli investimenti, della ricerca e innovazione, delle PMI e del mercato unico;

- una consultazione pubblica online, della durata di 12 settimane, avviata nel 2017 per raccogliere le opinioni di un pubblico più vasto (circa 90 partecipanti) sulla valutazione e sul riesame dell'ENISA;
- una consultazione pubblica online, della durata di 12 settimane, svoltasi nel 2016 in occasione dell'avvio del partenariato pubblico-privato contrattuale sulla cibersicurezza (circa 240 partecipanti).

La Commissione ha inoltre organizzato consultazioni mirate su questa iniziativa, con seminari, riunioni e richieste mirate di collaborazione (da parte dell'ENISA e dell'Agenzia europea per la difesa). Il periodo di consultazione si è protratto per 6 mesi, dal novembre 2017 fino al marzo 2018. La Commissione ha inoltre condotto una mappatura dei centri di competenze, che ha permesso di raccogliere i contributi di 665 centri nel settore della cibersicurezza in merito alle rispettive conoscenze, alle attività, agli ambiti operativi e alla cooperazione internazionale. L'indagine è stata avviata a gennaio. Sono stati presi in considerazione ai fini dell'analisi della relazione gli studi presentati entro l'8 marzo 2018.

Secondo i portatori di interessi delle comunità dell'industria e della ricerca, il Centro di competenza e la rete potrebbero conferire un valore aggiunto agli sforzi attuali a livello nazionale, contribuendo alla creazione di un ecosistema di cibersicurezza europeo che consenta di migliorare la cooperazione tra le comunità dell'industria e della ricerca. Tali portatori di interessi hanno inoltre affermato di ritenere necessario che l'UE e gli Stati membri adottino una pianificazione strategica attiva a lungo termine, per quanto concerne la politica industriale in materia di sicurezza informatica, che si spinga al di là dell'ambito della ricerca e dell'innovazione. Hanno altresì espresso l'esigenza di accedere a capacità essenziali quali strutture di prova e sperimentazione e di nutrire maggiori ambizioni per quanto riguarda il superamento del divario di competenze in materia di cibersicurezza, per esempio mediante progetti europei su vasta scala per attrarre i talenti migliori. Tutti gli aspetti sopra menzionati sono inoltre ritenuti necessari affinché l'Unione venga riconosciuta a livello mondiale tra i leader nel campo della sicurezza informatica.

Gli Stati membri, nel quadro delle attività di consultazione svolte a partire dallo scorso settembre[15] e nelle conclusioni in proposito del Consiglio[16] hanno accolto con favore l'intenzione di istituire una rete di competenza per la cibersicurezza al fine di stimolare lo sviluppo e l'implementazione di tecnologie nella cibersicurezza, sottolineando l'esigenza di adottare un approccio inclusivo nei confronti di tutti gli Stati membri e dei relativi centri di eccellenza e competenza e di prestare particolare attenzione alla complementarità. Nello specifico, per quanto riguarda il futuro Centro di competenza, gli Stati membri hanno evidenziato l'importanza del suo ruolo di coordinamento a supporto della rete. In particolare, relativamente alle attività e alle esigenze nazionali di ciberdifesa, con la mappatura delle esigenze degli Stati membri nel campo della ciberdifesa, eseguita nel marzo 2018 dal Servizio europeo per l'azione esterna, si è visto che la maggior parte degli Stati membri individua il valore aggiunto nel sostegno dell'UE all'istruzione e alla formazione nel campo della ciberdifesa e al sostegno dell'industria attraverso le attività di ricerca e sviluppo[17]. L'iniziativa verrebbe infatti attuata insieme agli Stati membri o ad enti da essi finanziati. Le collaborazioni tra le comunità dell'industria, della ricerca e/o del settore pubblico riunirebbero e

15 Per esempio la tavola rotonda ad alto livello con gli Stati Membri (vicepresidente Ansip, commissario Gabriel), del 5 dicembre 2017.

16 Consiglio "Affari generali": conclusioni del Consiglio sulla comunicazione congiunta al Parlamento europeo al Consiglio: Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE (20 novembre 2017).

17 SEAE, marzo 2018.

consoliderebbero gli enti attuali e gli sforzi per non crearne di nuovi. Gli Stati membri sarebbero inoltre impegnati nella definizione di azioni specifiche destinate al settore pubblico in quanto utente diretto della tecnologia e delle competenze in materia di cibersicurezza.

- **Valutazione d'impatto**

L'11 aprile 2017 è stata sottoposta al comitato per il controllo normativo una valutazione d'impatto a sostegno della presente iniziativa, che ha ricevuto un parere positivo con riserve. La valutazione d'impatto è stata successivamente rivista alla luce delle osservazioni del comitato; il parere del comitato e l'allegato in cui sono analizzate le osservazioni del comitato sono pubblicati insieme alla presente proposta.

Nella valutazione d'impatto sono state prese in considerazione alcune opzioni strategiche, sia legislative che non legislative. Le opzioni seguenti sono state selezionate per un esame approfondito:

- lo scenario di base (opzione collaborativa) presuppone la continuazione dell'approccio attuale allo sviluppo di capacità industriali e tecnologiche in materia di cibersicurezza nell'UE, attraverso il sostegno alla ricerca e all'innovazione e meccanismi di collaborazione correlati previsti dal 9° programma quadro;
- opzione 1: rete di competenza per la cibersicurezza con un Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, con il doppio mandato di perseguire l'attuazione di misure a supporto delle tecnologie industriali e nell'ambito della ricerca e dell'innovazione;
- opzione 2: rete di competenza per la cibersicurezza con un centro europeo di ricerca e di competenza in materia e l'obiettivo di occuparsi di attività di ricerca e innovazione.

Nella fase iniziale sono state scartate le seguenti opzioni: 1) l'assenza di qualsiasi intervento; 2) l'opzione di istituire solo la rete di competenza per la cibersicurezza; 3) l'opzione di creare solo una struttura centralizzata e 4) l'opzione di avvalersi di un'agenzia esistente, l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), l'Agenzia esecutiva per la ricerca (REA) o l'Agenzia esecutiva per l'innovazione e le reti (INEA).

Nell'analisi si è concluso che l'opzione 1 è quella più adatta per raggiungere gli obiettivi dell'iniziativa, offrendo nel contempo i migliori risultati in termini economici, sociali e ambientali e salvaguardando gli interessi dell'Unione. Questi i principali argomenti a favore di tale opzione: la possibilità di dare vita a una vera politica industriale in materia di sicurezza informatica, sostenendo attività connesse non solo alla ricerca e allo sviluppo, ma anche alla diffusione sul mercato; la flessibilità per consentire l'adozione di diversi modelli di cooperazione con la rete di centri di competenza per ottimizzare l'impiego delle conoscenze e delle risorse esistenti; la possibilità di strutturare la cooperazione e gli impegni assunti congiuntamente dalle parti interessate pubbliche e private di tutti i settori pertinenti, tra cui la difesa. Da ultimo, l'opzione 1 permette anche di aumentare le sinergie e può fungere da meccanismo di attuazione per due diversi flussi di finanziamento dell'UE per la cibersicurezza nell'ambito del prossimo quadro finanziario pluriennale (programmi Europa digitale e Orizzonte Europa).

- **Diritti fondamentali**

Questa iniziativa permetterà alle autorità pubbliche e alle imprese di tutti gli Stati membri di prevenire le minacce cibernetiche e di reagire ad esse in modo più efficace attraverso l'offerta e l'adozione di soluzioni e prodotti più sicuri. In particolare, ciò è rilevante per la protezione dell'accesso a servizi essenziali (per esempio trasporti e servizi sanitari, bancari e finanziari).

Inoltre è probabile che un aumento della capacità dell'Unione europea di garantire i propri prodotti e servizi aiuterà i cittadini a godere dei loro diritti e dei valori democratici (per esempio tutelando meglio i loro diritti relativi alle informazioni sanciti dalla Carta dei diritti fondamentali, in particolare il diritto alla vita privata e alla protezione dei dati di personali) e, di conseguenza, ad accrescere la loro fiducia nella società e nell'economia digitali.

4. INCIDENZA SUL BILANCIO

Il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, in cooperazione con la rete di competenza per la cibersicurezza, costituirà il principale organo esecutivo per le risorse finanziarie dell'Unione dedicate alla cibersicurezza nell'ambito dei programmi Europa digitale e Orizzonte Europa.

Le implicazioni di bilancio relative all'attuazione di Europa digitale sono elencate dettagliatamente nella scheda finanziaria legislativa allegata alla presente proposta. Nel corso del processo legislativo e, in ogni caso, prima che venga raggiunto un accordo politico, la Commissione proporrà il contributo proveniente dalla dotazione finanziaria del polo tematico "Società inclusiva e sicura" del pilastro II, "Sfide globali e competitività industriale" di Orizzonte Europa (una dotazione complessiva di 2 800 000 000 EUR) di cui all'articolo 21, paragrafo 1, lettera b). La proposta si baserà sull'esito del processo di pianificazione strategica definito all'articolo 6, paragrafo 6, del regolamento XXX [programma quadro di Orizzonte Europa].

5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

La presente proposta prevede esplicitamente (all'articolo 38) una clausola di valutazione, con cui la Commissione eseguirà una valutazione indipendente. Successivamente la Commissione riferirà al Parlamento europeo e al Consiglio sulla sua valutazione corredata, se del caso, di una proposta per il riesame, al fine di misurare l'impatto dell'atto giuridico e il suo valore aggiunto. Sarà applicata la metodologia di valutazione della Commissione volta a "Legiferare meglio".

A norma dell'articolo 17 della presente proposta, ogni due anni il direttore esecutivo dovrebbe presentare al consiglio di direzione una valutazione ex post delle attività della rete e del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza. Inoltre, il direttore esecutivo dovrebbe elaborare un piano d'azione volto a dare seguito alle conclusioni delle valutazioni retrospettive e riferire ogni due anni alla Commissione sui progressi compiuti. Il consiglio di direzione dovrebbe essere responsabile del monitoraggio dell'adeguatezza del seguito dato a tali conclusioni, ai sensi dell'articolo 16 della presente proposta.

Presunti casi di cattiva amministrazione nelle attività dell'organo giuridico possono formare oggetto di indagini da parte del Mediatore europeo ai sensi dell'articolo 228 del trattato.

2018/0328 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento

Contributo della Commissione europea per la riunione dei leader del 19-20 settembre 2018 a Salisburgo

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 173, paragrafo 3, e l'articolo 188, primo comma,

vista la proposta della Commissione europea,

visto il parere del Comitato economico e sociale europeo[18],

visto il parere del Comitato delle regioni[19],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) la nostra vita quotidiana e le nostre economie dipendono sempre di più dalle tecnologie digitali e i cittadini sono sempre più esposti a gravi incidenti informatici. La sicurezza futura dipende anche dal potenziamento della capacità tecnologica e industriale di proteggere l'Unione europea dalle minacce informatiche, in quanto sia le infrastrutture civili che le capacità militari devono poter fare affidamento su sistemi digitali sicuri.

(2) L'Unione ha costantemente intensificato le sue attività per far fronte alle crescenti sfide in materia di sicurezza informatica, in conformità alla strategia per la cibersicurezza del 2013[20] intesa a promuovere un ecosistema cibernetico affidabile, sicuro e aperto. Nel 2016 l'Unione ha adottato le prime misure nel settore della cibersicurezza attraverso la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio[21] sulla sicurezza delle reti e dei sistemi informativi.

---

18 GU C […] del […], pag. […].

19 GU C […] del […], pag. […].

20 Comunicazione congiunta al Parlamento europeo e al Consiglio: Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro, JOIN(2013) 1 final.

21 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

(3) Nel settembre 2017 la Commissione e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato la comunicazione congiunta[22] "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE" per rafforzare ulteriormente la resilienza, la deterrenza e la risposta dell'Unione agli attacchi informatici.

(4) In occasione del vertice di Tallinn sul digitale del settembre 2017, i capi di Stato e di governo hanno invitato l'Unione a diventare "un leader mondiale della cibersicurezza entro il 2025, al fine di garantire la fiducia, la sicurezza e la tutela dei nostri cittadini, dei nostri consumatori e delle nostre imprese online e di fare sì che Internet sia libero e regolamentato".

(5) Una grave perturbazione delle reti e dei sistemi informativi può ripercuotersi su singoli Stati membri e su tutta l'Unione. La sicurezza delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno. Al momento l'Unione dipende da fornitori di sicurezza informatica non europei. Tuttavia, è nell'interesse strategico dell'UE garantire il mantenimento e lo sviluppo di capacità tecnologiche essenziali in materia di sicurezza informatica per tutelare il proprio mercato unico digitale, e in particolare per proteggere reti e sistemi informativi critici e fornire servizi fondamentali di cibersicurezza.

(6) L'Unione vanta grandi competenze ed esperienza nello sviluppo industriale, nella tecnologia e nella ricerca sulla cibersicurezza, ma gli sforzi delle comunità dell'industria e della ricerca sono frammentati, disallineati e privi di una progettualità comune, il che frena la competitività in questo ambito. Tali sforzi e competenze devono essere aggregati, collegati in rete e impiegati in modo efficiente per consolidare e integrare le attuali capacità tecnologiche, industriali e di ricerca a livello nazionale e di Unione.

(7) Con le conclusioni adottate nel novembre 2017, il Consiglio ha sollecitato la Commissione a fornire rapidamente una valutazione d'impatto sulle opzioni possibili per creare una rete di centri di competenza per la cibersicurezza con il Centro europeo di ricerca e di competenza e a proporre entro la metà del 2018 lo strumento giuridico pertinente.

(8) Il Centro di competenza dovrebbe costituire il principale strumento dell'Unione per concentrare gli investimenti nello sviluppo industriale, nella tecnologia e nella ricerca sulla cibersicurezza e per attuare progetti e iniziative pertinenti in collaborazione con la rete di competenza per la cibersicurezza. Oltre a fornire il sostegno finanziario legato alla sicurezza informatica e concesso dai programmi Europa digitale e Orizzonte Europa, il Centro dovrebbe essere aperto al Fondo europeo di sviluppo regionale e ad altri programmi, ove opportuno. Questo approccio dovrebbe contribuire alla creazione di sinergie e al coordinamento del sostegno finanziario connesso allo sviluppo industriale, all'innovazione, alla tecnologia e alla ricerca sulla cibersicurezza, evitando le duplicazioni.

(9) Considerando che gli obiettivi di questa iniziativa possono essere conseguiti al meglio se vi aderiscono tutti gli Stati membri o il maggior numero di Stati membri possibile, e al fine di incentivare la loro partecipazione, solo gli Stati membri che contribuiscono

[22] Comunicazione congiunta al Parlamento europeo e al Consiglio "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE", JOIN(2017) 450 final.

finanziariamente ai costi amministrativi e operativi del Centro di competenza dovrebbero detenere il diritto di voto.

(10) La partecipazione finanziaria degli Stati membri che aderiscono dovrebbe essere commisurata al contributo finanziario dell'Unione a favore di questa iniziativa.

(11) Il Centro di competenza dovrebbe agevolare l'attività della rete di competenza per la cibersicurezza ("la rete"), costituita da centri nazionali di coordinamento in ciascuno Stato membro, e contribuire a coordinarla. I centri nazionali di coordinamento dovrebbero ricevere il sostegno finanziario diretto dell'Unione, ivi comprese sovvenzioni concesse in assenza di un invito a presentare proposte, al fine di svolgere attività connesse al presente regolamento.

(12) I centri nazionali di coordinamento devono essere selezionati dagli Stati membri. Oltre alla capacità amministrativa necessaria, i centri devono disporre di competenze tecnologiche in materia di cibersicurezza o devono potervi accedere direttamente, in particolare in ambiti quali la crittografia, i servizi di sicurezza delle TIC, la rilevazione automatica di intrusioni, la sicurezza dei sistemi, delle reti, del software e delle applicazioni e gli aspetti umani e sociali della sicurezza e della privacy. Inoltre devono essere in grado di interagire e di coordinarsi efficacemente con l'industria, il settore pubblico, fra cui le autorità designate a norma della direttiva 2016/1148 del Parlamento europeo e del Consiglio[23] e la comunità della ricerca.

(13) Qualora sia fornito sostegno finanziario a centri nazionali di coordinamento al fine di assistere terzi a livello nazionale, tale sostegno deve essere trasmesso ai portatori di interessi pertinenti attraverso convenzioni di sovvenzione a cascata.

(14) Tecnologie emergenti come l'intelligenza artificiale, l'Internet delle cose, il calcolo ad alte prestazioni (High-Performance Computing - HPC) e l'informatica quantistica, la blockchain e concetti come le identità digitali sicure creano nuove sfide per la cibersicurezza e offrono nel contempo alcune soluzioni. La valutazione e la convalida dell'affidabilità di sistemi TIC esistenti e futuri richiederanno la sperimentazione di soluzioni di sicurezza contro gli attacchi nei confronti di macchine HPC e quantistiche. Il Centro di competenza, la rete e la comunità delle competenze in materia di cibersicurezza dovrebbero contribuire al progresso e alla diffusione delle soluzioni più recenti nel campo della cibersicurezza. Contestualmente, il Centro di competenza e la rete dovrebbero essere al servizio di sviluppatori e operatori in settori critici quali i trasporti, l'energia, la sanità, le finanze, l'amministrazione, le telecomunicazioni, la manifattura, la difesa e lo spazio per aiutarli a risolvere i loro problemi di cibersicurezza.

(15) Il Centro di competenza dovrebbe avere diverse funzioni chiave. In primo luogo, dovrebbe agevolare e contribuire a coordinare l'attività della rete europea di competenza per la cibersicurezza e promuovere la comunità delle competenze in materia di cibersicurezza. Il Centro dovrebbe guidare l'agenda tecnologica della cibersicurezza e facilitare l'accesso alle competenze raccolte nella rete e nella comunità delle competenze in materia di cibersicurezza. In secondo luogo, dovrebbe attuare le parti pertinenti dei programmi Europa digitale e Orizzonte Europa assegnando sovvenzioni, in genere in seguito ad un invito a presentare proposte. In

[23] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

terzo luogo, il Centro di competenza dovrebbe agevolare gli investimenti congiunti da parte dell'Unione, degli Stati membri e/o dell'industria.

(16) Il Centro di competenza dovrebbe stimolare e sostenere la cooperazione e il coordinamento delle attività della comunità delle competenze in materia di cibersicurezza, coinvolgendo un gruppo vasto, aperto e diversificato di operatori impegnati nella tecnologia della cibersicurezza. Tale comunità dovrebbe includere in particolare enti di ricerca, industrie sul versante dell'offerta e su quello della domanda, nonché il settore pubblico. La comunità delle competenze in materia di cibersicurezza dovrebbe fornire il proprio contributo alle attività e al piano di lavoro del Centro di competenza, oltre a beneficiare delle attività di creazione di comunità del Centro di competenza e della rete, ma non dovrebbe essere privilegiata in altro modo per quanto riguarda gli inviti a presentare proposte o gli inviti a presentare offerte.

(17) Al fine di rispondere alle esigenze delle industrie tanto sul versante della domanda quanto su quello dell'offerta, per il compito del Centro di competenza, ossia fornire alle imprese conoscenze e assistenza tecnica in tema di cibersicurezza, occorrerebbe tenere conto sia dei prodotti e dei servizi delle TIC sia di tutti gli altri prodotti e soluzioni industriali e tecnologici in cui deve essere integrata la cibersicurezza.

(18) Considerando che il Centro di competenza e la rete dovrebbero cercare di realizzare sinergie tra la sfera civile e quella relativa alla difesa della cibersicurezza, i progetti finanziati dal programma Orizzonte europea saranno attuati in conformità del regolamento XXX [regolamento su Orizzonte Europa], secondo cui le attività di ricerca e innovazione svolte nell'ambito di tale programma riguardano le applicazioni civili.

(19) Ai fini di una collaborazione strutturata e sostenibile, il rapporto tra il Centro di competenza e i centri nazionali di coordinamento dovrebbe basarsi su un accordo contrattuale.

(20) Dovrebbero essere adottate disposizioni opportune per garantire la responsabilità e la trasparenza del Centro di competenza.

(21) Alla luce delle rispettive competenze in tema di cibersicurezza, il Centro comune di ricerca della Commissione e l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) dovrebbero svolgere un ruolo attivo nella comunità delle competenze in materia di cibersicurezza e nel consiglio consultivo industriale e scientifico.

(22) Qualora ricevano un contributo finanziario dal bilancio generale dell'Unione, i centri nazionali di coordinamento e gli enti che fanno parte della comunità delle competenze in materia di cibersicurezza dovrebbero pubblicizzare il fatto che le rispettive attività si svolgono nel contesto della presente iniziativa.

(23) Il contributo dell'Unione a favore del Centro di competenza dovrebbe finanziare la metà dei costi legati all'istituzione e alle attività amministrative e di coordinamento del Centro di competenza. Al fine di evitare il doppio finanziamento, tali attività non dovrebbero beneficiare contemporaneamente di un contributo proveniente da altri programmi dell'Unione.

(24) Il consiglio di direzione del Centro di competenza, composto dagli Stati membri e dalla Commissione, dovrebbe definire l'orientamento generale delle operazioni del Centro di competenza e garantire che quest'ultimo svolga i propri compiti conformemente al presente regolamento. Il consiglio di direzione dovrebbe godere dei poteri necessari per formare il bilancio, verificarne l'esecuzione, adottare l'opportuna

regolamentazione finanziaria, stabilire procedure operative trasparenti per l'iter decisionale del Centro di competenza, adottare il piano di lavoro e il piano strategico pluriennale del Centro di competenza nel rispetto delle priorità di conseguimento dei suoi obiettivi e delle sue funzioni, adottare il suo regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione del suo mandato e in merito alla sua conclusione.

(25) Per garantire il funzionamento corretto ed efficace del Centro di competenza, la Commissione e gli Stati membri dovrebbero assicurare che le persone da nominare nel consiglio di direzione dispongano di competenze ed esperienze professionali adeguate nelle aree funzionali. La Commissione e gli Stati membri dovrebbero inoltre sforzarsi di limitare l'avvicendamento dei loro rispettivi rappresentanti nel consiglio di direzione, per assicurare la continuità dei lavori.

(26) Il corretto funzionamento del Centro di competenza esige che il direttore esecutivo sia nominato in base ai meriti e alla comprovata esperienza amministrativa e manageriale, nonché alla competenza e all'esperienza acquisita in materia di cibersicurezza, e che le sue funzioni siano svolte in completa indipendenza.

(27) È opportuno che il Centro di competenza disponga di un consiglio consultivo industriale e scientifico come organo consultivo per garantire un dialogo periodico con il settore privato, le organizzazioni dei consumatori e gli altri soggetti interessati. Il consiglio consultivo industriale e scientifico dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione del consiglio di direzione del Centro di competenza. La composizione del consiglio consultivo industriale e scientifico e i compiti ad esso assegnati, quali la consulenza in merito al piano di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dal Centro di competenza.

(28) Il Centro di competenza dovrebbe beneficiare della particolare esperienza e dell'ampia e significativa rappresentanza dei portatori di interessi, acquisite attraverso il partenariato pubblico-privato contrattuale sulla cibersicurezza nel corso di Orizzonte 2020, tramite il suo consiglio consultivo industriale e scientifico.

(29) Il Centro di competenza dovrebbe disporre di norme relative alla prevenzione e alla gestione dei conflitti di interessi. Dovrebbe inoltre applicare le disposizioni pertinenti dell'Unione in materia di accesso del pubblico ai documenti stabilite dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio[24]. Il trattamento dei dati personali da parte del Centro di competenza sarà soggetto al regolamento (UE) n. XXX/2018 del Parlamento europeo e del Consiglio. È opportuno che il Centro di competenza si conformi alle disposizioni applicabili alle istituzioni dell'Unione e alla legislazione nazionale in materia di gestione delle informazioni, in particolare delle informazioni sensibili non classificate e delle informazioni classificate dell'UE.

(30) È opportuno che gli interessi finanziari dell'Unione e degli Stati membri siano tutelati durante l'intero ciclo di spesa attraverso misure proporzionate, come la prevenzione e l'individuazione di irregolarità, lo svolgimento di indagini sulle stesse, il recupero dei fondi perduti, indebitamente versati o non correttamente utilizzati e, se del caso, attraverso l'applicazione di sanzioni amministrative e finanziarie, in conformità al

[24] Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

regolamento (UE, Euratom) XXX del Parlamento europeo e del Consiglio[25] [il regolamento finanziario].

(31) Il Centro di competenza dovrebbe operare in modo aperto e trasparente fornendo tempestivamente tutte le informazioni pertinenti e promuovendo le proprie attività, incluse le attività di informazione e divulgazione destinate al pubblico. Il regolamento interno degli organi del Centro di competenza dovrebbe essere reso pubblico.

(32) È opportuno che il revisore contabile interno della Commissione eserciti nei confronti del Centro di competenza le stesse competenze esercitate nei confronti della Commissione.

(33) La Commissione, il Centro di competenza, la Corte dei conti e l'Ufficio europeo per la lotta antifrode dovrebbero avere accesso a tutte le informazioni necessarie e ai locali per eseguire controlli e svolgere indagini sulle sovvenzioni, gli appalti e gli accordi firmati dal Centro di competenza.

(34) Poiché gli obiettivi del presente regolamento, vale a dire mantenere e sviluppare le capacità tecnologiche e industriali dell'Unione in materia di cibersicurezza, aumentare la competitività del settore della sicurezza informatica dell'UE e trasformare la cibersicurezza in un vantaggio competitivo per altri settori dell'Unione, non possono essere conseguiti in misura sufficiente dagli Stati membri a causa della dispersione delle limitate risorse e delle dimensioni dell'investimento necessario, ma possono essere conseguiti meglio a livello di Unione a motivo della necessità di evitare inutili sovrapposizioni, contribuendo al raggiungimento di una massa critica e garantendo l'utilizzo ottimale dei finanziamenti pubblici, l'Unione può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI E PRINCIPI DEL CENTRO DI COMPETENZA E DELLA RETE

Articolo 1

Oggetto

1. Il presente regolamento istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza (il "Centro di competenza") e la rete dei centri nazionali di coordinamento, oltre a stabilire le modalità di nomina dei centri nazionali di coordinamento e di istituzione della comunità delle competenze in materia di cibersicurezza.

2. Il Centro di competenza contribuisce all'attuazione della parte relativa alla cibersicurezza del programma Europa digitale, istituito dal regolamento n. XXX e, in particolare, delle azioni di cui all'articolo 6 del regolamento (UE) n. XXX [programma Europa digitale] e del programma Orizzonte Europa, istituito dal

[25] [aggiungere titolo e riferimento GU]

regolamento n. XXX, in particolare dal pilastro II, sezione 2.2.6, dell'allegato I della decisione n. XXX relativa all'istituzione del programma specifico di attuazione di Orizzonte Europa - il programma quadro di ricerca e innovazione [n. di riferimento del programma specifico].

3. Il Centro di competenza ha sede a [Bruxelles, Belgio].

4. Il Centro di competenza ha personalità giuridica. In ogni Stato membro esso gode della più ampia capacità giuridica riconosciuta alle persone giuridiche dalla legislazione di tale Stato. In particolare, può acquisire o alienare beni mobili e immobili e stare in giudizio.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

1) "cibersicurezza": protezione della rete e dei sistemi informativi, dei loro utenti e di altre persone dalle minacce informatiche;

2) "prodotti e soluzioni per la cibersicurezza": prodotti, servizi o processi TIC con la finalità specifica di proteggere la rete e i sistemi informativi, i loro utenti e le persone interessate dalle minacce informatiche;

3) "autorità pubblica": ogni governo o altra amministrazione pubblica, compresi gli organi consultivi pubblici a livello nazionale, regionale o locale, oppure ogni persona fisica o giuridica che svolge funzioni pubbliche ai sensi della legislazione nazionale, compresi incarichi specifici;

4) "Stato membro partecipante": Stato membro che contribuisce finanziariamente di propria volontà ai costi amministrativi e operativi del Centro di competenza.

Articolo 3

Missione del Centro e della rete

1. Il Centro di competenza e la rete aiutano l'Unione a:

   a) mantenere e sviluppare le capacità tecnologiche e industriali in materia di cibersicurezza necessarie a tutelare il proprio mercato unico digitale;

   b) aumentare la competitività nel settore della sicurezza informatica dell'UE e trasformare la cibersicurezza in un vantaggio competitivo per altri settori dell'Unione.

2. Il Centro di competenza svolge i propri compiti, se del caso, in collaborazione con la rete dei centri nazionali di coordinamento e la comunità delle competenze in materia di cibersicurezza.

Articolo 4

Obiettivi e compiti del Centro

Il Centro di competenza ha i seguenti obiettivi e le seguenti funzioni:

1. agevolare e contribuire a coordinare l'attività della rete dei centri nazionali di coordinamento ("la rete") di cui all'articolo 6 e della comunità delle competenze in materia di cibersicurezza di cui all'articolo 8;

2. contribuire all'attuazione della parte relativa alla cibersicurezza del programma Europa digitale, istituito dal regolamento n. XXX[26] e, in particolare, delle azioni di cui all'articolo 6 del regolamento (UE) n. XXX [programma Europa digitale] e del programma Orizzonte Europa, istituito dal regolamento n. XXX[27], in particolare dal pilastro II, sezione 2.2.6, dell'allegato I della decisione n. XXX relativa all'istituzione del programma specifico di attuazione di Orizzonte Europa - il programma quadro di ricerca e innovazione [n. di riferimento del programma specifico] e di altri programmi dell'UE [ove previsto dagli atti giuridici dell'Unione];

3. rafforzare le capacità, le conoscenze e le infrastrutture in materia di cibersicurezza al servizio delle imprese, del settore pubblico e delle comunità della ricerca, attraverso lo svolgimento delle seguenti funzioni:

    a) tenendo conto delle infrastrutture industriali e di ricerca d'avanguardia e dei relativi servizi nell'ambito della cibersicurezza, acquisire e potenziare tali infrastrutture e servizi e renderli funzionanti e disponibili per un'ampia gamma di utilizzatori del settore in tutta l'Unione, comprese le PMI, il settore pubblico, la comunità scientifica e quella della ricerca;

    b) tenendo conto delle infrastrutture industriali e di ricerca d'avanguardia e dei relativi servizi nell'ambito della cibersicurezza, fornire assistenza ad altri enti, anche a livello finanziario, per acquisire e potenziare tali infrastrutture e servizi e renderli funzionanti e disponibili per un'ampia gamma di utilizzatori del settore in tutta l'Unione, comprese le PMI, il settore pubblico, la comunità scientifica e quella della ricerca;

    c) divulgare conoscenze e fornire assistenza tecnica in tema di cibersicurezza all'industria e alle autorità pubbliche, in particolare promuovendo azioni volte ad agevolare l'accesso alle competenze disponibili presso la rete e la comunità delle competenze in materia di cibersicurezza;

4. contribuire a un'ampia implementazione dei prodotti e delle soluzioni all'avanguardia per la sicurezza informatica in tutti i settori economici, svolgendo le seguenti funzioni:

    a) stimolare la ricerca e lo sviluppo nell'ambito della cibersicurezza e la diffusione di prodotti e soluzioni per la sicurezza informatica dell'Unione presso le autorità pubbliche e i settori utilizzatori;

    b) assistere le autorità pubbliche, le industrie sul versante della domanda e altri utilizzatori nell'adozione e nell'integrazione delle soluzioni più recenti nel campo della sicurezza informatica;

    c) sostenere in particolare le autorità pubbliche nell'organizzazione dei loro appalti pubblici o condurre appalti per l'acquisizione di prodotti e soluzioni all'avanguardia per la sicurezza informatica a nome di autorità pubbliche;

    d) fornire assistenza tecnica e finanziaria alle start-up e alle PMI nel settore della cibersicurezza affinché accedano a mercati potenziali e attraggano investimenti;

---

26 [aggiungere il titolo completo e il riferimento alla GU]

27 [aggiungere il titolo completo e il riferimento alla GU]

5. migliorare la comprensione della sicurezza informatica e contribuire a ridurre i divari di competenze presenti nell'Unione in merito a tale settore operando come segue:

    a) promuovendo l'ulteriore sviluppo delle competenze in materia di cibersicurezza, se del caso insieme ad agenzie e organi competenti dell'UE, tra cui l'ENISA;

6. contribuire al consolidamento della ricerca e dello sviluppo nel campo della cibersicurezza nell'Unione, attraverso:

    a) la fornitura di assistenza finanziaria a favore delle attività di ricerca nel settore della cibersicurezza seguendo un'agenda strategica pluriennale comune, industriale, tecnologica e di ricerca che sia costantemente sottoposta a valutazioni e a miglioramenti;

    b) il sostegno alla ricerca su vasta scala e a progetti dimostrativi riguardanti le capacità tecnologiche di prossima generazione in materia di cibersicurezza, in collaborazione con l'industria e con la rete;

    c) il sostegno alla ricerca e all'innovazione per la standardizzazione della tecnologia della cibersicurezza;

7. potenziare la cooperazione tra la sfera civile e quella relativa alla difesa per quanto concerne tecnologie e applicazioni a duplice uso nel campo della cibersicurezza, operando come segue:

    a) sostenendo gli Stati membri e i rappresentanti dell'industria e della ricerca per quanto riguarda la ricerca, lo sviluppo e l'implementazione;

    b) contribuendo alla cooperazione tra Stati membri grazie alla promozione dell'istruzione, della formazione e delle esercitazioni;

    c) riunendo i portatori di interesse, grazie alla promozione delle sinergie tra la ricerca e i mercati della cibersicurezza civile e per la difesa;

8. potenziare le sinergie tra le dimensioni civile e di difesa della cibersicurezza in relazione al Fondo europeo per la difesa, operando come segue:

    a) fornendo consulenza, condividendo le conoscenze e agevolando la collaborazione fra i portatori di interessi;

    b) gestendo progetti multinazionali di ciberdifesa, qualora richiesto dagli Stati membri, agendo così da responsabile del progetto ai sensi del regolamento XXX [regolamento che istituisce il Fondo europeo per la difesa].

Articolo 5

Investimenti in infrastrutture, capacità, prodotti o soluzioni e relativo utilizzo

1. Qualora il Centro di competenza fornisca finanziamenti per infrastrutture, capacità, prodotti o soluzioni a norma dell'articolo 4, paragrafi 3 e 4, sotto forma di sovvenzione o di premio, il piano di lavoro del Centro di competenza può specificare in particolare:

    a) norme per disciplinare la gestione di un'infrastruttura o una capacità, tra cui, ove opportuno, l'affidamento di tale gestione a un soggetto ospitante sulla base di criteri definiti dal Centro di competenza;

b) norme per disciplinare l'accesso a un'infrastruttura o una capacità e il relativo utilizzo.

2. Il Centro di competenza può essere responsabile dell'esecuzione generale di azioni congiunte pertinenti in materia di appalti, ivi compresi appalti pre-commerciali a nome di membri della rete, membri della comunità delle competenze in materia di cibersicurezza o terzi in rappresentanza degli utilizzatori di prodotti e soluzioni per la sicurezza informatica. A tale fine, il Centro di competenza può essere assistito da uno o più centri nazionali di coordinamento o membri della comunità delle competenze in materia di cibersicurezza.

Articolo 6

Nomina dei centri nazionali di coordinamento

1. Entro il [data], ciascuno Stato membro nomina l'ente che agisce da centro nazionale di coordinamento ai fini del presente regolamento e ne informa la Commissione.

2. Sulla base di una valutazione relativa alla conformità di tale ente ai criteri di cui al paragrafo 4, la Commissione adotta una decisione entro 6 mesi dalla data della nomina trasmessa dallo Stato membro, decisione con cui accredita l'ente in qualità di centro nazionale di coordinamento o respinge la nomina. L'elenco dei centri nazionali di coordinamento è pubblicato dalla Commissione.

3. Gli Stati membri possono nominare in qualsiasi momento un nuovo ente come centro nazionale di coordinamento ai fini del presente regolamento. I paragrafi 1 e 2 si applicano alla nomina di qualsiasi nuovo ente.

4. Il centro nazionale di coordinamento nominato deve essere in grado di sostenere il Centro di competenza e la rete nell'adempimento della loro missione di cui all'articolo 3 del presente regolamento. I centri nazionali di coordinamento devono disporre di competenze tecnologiche in materia di cibersicurezza o devono potervi accedere direttamente, e devono essere in grado di interagire e coordinarsi efficacemente con l'industria, il settore pubblico e la comunità della ricerca.

5. Il rapporto tra il Centro di competenza e i centri nazionali di coordinamento si basa su un accordo contrattuale sottoscritto dal Centro di competenza e da ciascuno dei centri nazionali di coordinamento. L'accordo stabilisce le norme che disciplinano il rapporto e la divisione dei compiti tra il Centro di competenza e ciascun centro nazionale di coordinamento.

6. La rete dei centri nazionali di coordinamento è composta da tutti i centri nazionali di coordinamento nominati dagli Stati membri.

Articolo 7

Funzioni dei centri nazionali di coordinamento

1. I centri nazionali di coordinamento hanno le seguenti funzioni:

a) sostenere il Centro di competenza nel conseguimento dei suoi obiettivi e, in particolare, nel coordinamento della comunità delle competenze in materia di cibersicurezza;

b) agevolare la partecipazione ai progetti transfrontalieri dell'industria e di altri attori a livello di Stati membri;

c) contribuire, assieme al Centro di competenza, all'individuazione e al superamento di problemi industriali specifici per settore in materia di cibersicurezza;

d) agire da punto di contatto a livello nazionale per la comunità delle competenze in materia di cibersicurezza e il Centro di competenza;

e) cercare di creare sinergie con attività pertinenti a livello nazionale e regionale;

f) attuare azioni specifiche per le quali il Centro di competenza ha concesso sovvenzioni, anche attraverso la fornitura di sostegno finanziario a terzi, a norma dell'articolo 204 del regolamento XXX [il nuovo regolamento finanziario], alle condizioni specificate nelle convenzioni di sovvenzione pertinenti;

g) promuovere e divulgare i risultati dell'attività della rete, della comunità delle competenze in materia di cibersicurezza e del Centro di competenza a livello nazionale o regionale;

h) valutare le richieste di adesione alla comunità delle competenze in materia di cibersicurezza da parte di enti situati nello stesso Stato membro del Centro di coordinamento.

2. Ai fini della lettera f), il sostegno finanziario a terzi può essere fornito sotto una qualsiasi delle forme specificate all'articolo 125 del regolamento XXX [nuovo regolamento finanziario], anche sotto forma di somme forfettarie.

3. I centri nazionali di coordinamento possono ricevere una sovvenzione dall'Unione a norma dell'articolo 195, lettera d), del regolamento XXX [nuovo regolamento finanziario] in relazione all'espletamento delle funzioni stabilite dal presente articolo.

4. Se del caso, i centri nazionali di coordinamento cooperano mediante la rete al fine di svolgere le funzioni di cui al paragrafo 1, lettere a), b), c), e) e g).

Articolo 8

La comunità delle competenze in materia di cibersicurezza

1. La comunità delle competenze in materia di cibersicurezza contribuisce alla missione del Centro di competenza di cui all'articolo 3, consolidando e divulgando le competenze in tema di sicurezza informatica in tutta l'Unione.

2. La comunità delle competenze in materia di cibersicurezza è costituita da organizzazioni di ricerca industriali, accademiche e senza scopo di lucro, nonché da associazioni ed enti pubblici o altri enti che si occupano di questioni operative e tecniche. Riunisce i principali portatori di interessi per quanto concerne le capacità tecnologiche e industriali in materia di cibersicurezza nell'Unione, coinvolgendo i centri nazionali di coordinamento e le istituzioni e gli organismi competenti dell'Unione europea.

3. Solo enti istituiti all'interno dell'Unione possono essere accreditati in qualità di membri della comunità delle competenze in materia di cibersicurezza. Essi sono tenuti a dimostrare di possedere competenze relative alla cibersicurezza in merito ad almeno uno dei seguenti ambiti:

a) ricerca;

b) sviluppo industriale;

c) formazione e istruzione.

4. Il Centro di competenza accredita enti istituiti a norma del diritto nazionale quali membri della comunità delle competenze in materia di cibersicurezza dopo una valutazione effettuata dal centro nazionale di coordinamento dello Stato membro in cui l'ente è istituito, con la quale si verifica se l'ente soddisfa o meno i criteri di cui al paragrafo 3. Un accreditamento non è limitato nel tempo, ma può essere revocato in qualsiasi momento dal Centro di competenza se quest'ultimo o il centro nazionale di coordinamento pertinente ritengono che l'ente non soddisfi i criteri di cui al paragrafo 3 o rientri nel campo di applicazione delle disposizioni pertinenti di cui all'articolo 136 del regolamento XXX [nuovo regolamento finanziario].

5. Il Centro di competenza accredita organismi, agenzie e uffici competenti dell'Unione quali membri della comunità delle competenze in materia di cibersicurezza dopo aver valutato se l'ente soddisfa o meno i criteri di cui al paragrafo 3. Un accreditamento non è limitato nel tempo, ma può essere revocato in qualsiasi momento dal Centro di competenza se quest'ultimo ritiene che l'ente non soddisfi i criteri di cui al paragrafo 3 o rientri nel campo di applicazione delle disposizioni pertinenti di cui all'articolo 136 del regolamento XXX [nuovo regolamento finanziario].

6. I rappresentanti della Commissione possono partecipare ai lavori della comunità.

Articolo 9

Funzioni dei membri della comunità delle competenze in materia di cibersicurezza

I membri della comunità delle competenze in materia di cibersicurezza:

1) assistono il Centro di competenza nel conseguimento della missione e degli obiettivi di cui agli articoli 3 e 4 e, a tale fine, operano a stretto contatto con il Centro di competenza e i centri nazionali di coordinamento pertinenti;

2) partecipano ad attività promosse dal Centro di competenza e dai centri nazionali di coordinamento;

3) se del caso, partecipano ai gruppi di lavoro istituiti dal consiglio di direzione del Centro di competenza per svolgere attività specifiche previste dal piano di lavoro del Centro di competenza;

4) se del caso, assistono il Centro di competenza e i centri nazionali di coordinamento nella promozione di progetti specifici;

5) promuovono e divulgano i risultati pertinenti delle attività e dei progetti svolti nell'ambito della comunità.

Articolo 10

Cooperazione del Centro di competenza con istituzioni, organismi, uffici e agenzie dell'Unione

1. Il Centro di competenza coopera con istituzioni, organismi, uffici e agenzie pertinenti dell'Unione, tra cui l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, la squadra di pronto intervento informatico (CERT-EU), il Servizio europeo per l'azione esterna , il Centro comune di ricerca della Commissione, l'Agenzia esecutiva per la ricerca, l'Agenzia esecutiva per l'innovazione e le reti, il Centro europeo per la lotta alla criminalità informatica di Europol e l'Agenzia europea per la difesa.

2. Tale cooperazione si svolge nel quadro di accordi di lavoro che vengono sottoposti all'approvazione preventiva della Commissione.

CAPO II

ORGANIZZAZIONE DEL CENTRO DI COMPETENZA

Articolo 11

Membri e struttura

1. I membri del Centro di competenza sono l'Unione, rappresentata dalla Commissione, e gli Stati membri.
2. La struttura del Centro di competenza comprende:
   a) un consiglio di direzione, che svolge le funzioni di cui all'articolo 13;
   b) un direttore esecutivo, che svolge le funzioni di cui all'articolo 16;
   c) un consiglio consultivo industriale e scientifico, che svolge le funzioni di cui all'articolo 20.

SEZIONE I

CONSIGLIO DI DIREZIONE

Articolo 12

Composizione del consiglio di direzione

1. Il consiglio di direzione è composto da un rappresentante per ciascuno Stato membro e da cinque rappresentanti della Commissione, a nome dell'Unione.
2. Ciascun membro del consiglio di direzione ha un supplente che lo rappresenta in sua assenza.
3. I membri del consiglio di direzione e i loro supplenti sono nominati in base alle loro conoscenze in campo tecnologico e delle pertinenti competenze gestionali, amministrative e di bilancio. La Commissione e gli Stati membri si sforzano di limitare l'avvicendamento dei loro rappresentanti nel consiglio di direzione, al fine di assicurarne la continuità dei lavori. La Commissione e gli Stati membri mirano a conseguire una rappresentanza equilibrata tra uomini e donne nel consiglio di direzione.
4. La durata del mandato dei membri del consiglio di direzione e dei loro supplenti è di quattro anni. Il mandato è rinnovabile.
5. I membri del consiglio di direzione agiscono nell'interesse del Centro di competenza, salvaguardandone gli obiettivi e la missione, l'identità, l'autonomia e la coerenza in modo indipendente e trasparente.
6. La Commissione può invitare osservatori, fra cui rappresentanti di organismi, uffici e agenzie dell'Unione, a partecipare alle riunioni del consiglio di direzione.
7. L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) è un osservatore permanente nel consiglio di direzione.

Articolo 13

Funzioni del consiglio di direzione

1. Il consiglio di direzione assume la responsabilità generale dell'orientamento strategico e dell'operato del Centro di competenza e sovrintende alle sue attività.

2. Il consiglio di direzione adotta il proprio regolamento interno. Il regolamento prevede procedure specifiche per individuare ed evitare i conflitti di interessi e garantire la riservatezza di tutte le informazioni sensibili.

3. Il consiglio di direzione prende le decisioni strategiche necessarie, in particolare:

   a) adotta un piano strategico pluriennale, in cui sono indicate le principali priorità e iniziative previste dal Centro di competenza, compresa una stima del fabbisogno finanziario e delle fonti di finanziamento;

   b) adotta il piano di lavoro, i conti e il bilancio annuali, nonché la relazione di attività annuale del Centro di competenza, sulla base di una proposta del direttore esecutivo.

   c) adotta il regolamento finanziario specifico del Centro di competenza, conformemente all'[articolo 70 del regolamento finanziario];

   d) adotta una procedura di nomina del direttore esecutivo;

   e) adotta i criteri e le procedure di valutazione e accreditamento degli enti in qualità di membri della comunità delle competenze in materia di cibersicurezza;

   f) nomina il direttore esecutivo, lo destituisce, ne proroga il mandato, gli fornisce orientamenti e ne controlla l'operato; nomina il contabile;

   g) adotta il bilancio annuale del Centro di competenza, compresa la tabella dell'organico con l'indicazione del numero di agenti temporanei per gruppo di funzioni e per grado, nonché del numero di agenti contrattuali e di esperti nazionali distaccati espressi in equivalenti a tempo pieno;

   h) adotta norme in materia di conflitto di interessi;

   i) istituisce gruppi di lavoro comprendenti membri della comunità delle competenze in materia di cibersicurezza;

   j) nomina membri del consiglio consultivo industriale e scientifico;

   k) istituisce una funzione di revisione contabile a norma del regolamento delegato (UE) n. 1271/2013 della Commissione[28];

   l) promuove il Centro di competenza su scala mondiale, in modo da renderlo più attrattivo e da farne un organismo di eccellenza a livello mondiale nel settore della cibersicurezza;

   m) definisce la strategia di comunicazione del Centro di competenza, su raccomandazione del direttore esecutivo;

[28] Regolamento delegato (UE) n. 1271/2013 della Commissione, del 30 settembre 2013, che stabilisce il regolamento finanziario quadro degli organismi di cui all'articolo 208 del regolamento (UE, Euratom) n. 966/2012 del Parlamento europeo e del Consiglio (GU L 328 del 7.12.2013, pag. 42).

n) è responsabile del monitoraggio dell'adeguatezza del seguito dato alle conclusioni delle valutazioni retrospettive;

o) se del caso, adotta modalità di applicazione dello statuto dei funzionari e del regime applicabile agli altri agenti conformemente all'articolo 31, paragrafo 3;

p) se del caso, adotta regole per il distacco di esperti nazionali presso il Centro di competenza e per il ricorso a tirocinanti conformemente all'articolo 32, paragrafo 2;

q) adotta norme di sicurezza per il Centro di competenza;

r) adotta una strategia antifrode, proporzionata ai rischi di frode, tenendo conto dei costi e dei benefici delle misure da attuare;

s) adotta la metodologia per il calcolo del contributo finanziario degli Stati membri;

t) è responsabile di tutti i compiti non espressamente attribuiti a un particolare organo del Centro di competenza; può assegnare tali compiti a qualsiasi organo del Centro di competenza.

Articolo 14

Presidente e riunioni del consiglio di direzione

1. Il consiglio di direzione elegge un presidente e un vicepresidente tra i membri con diritto di voto, per un periodo di due anni. Il mandato del presidente e del vicepresidente può essere prorogato una sola volta, previa decisione del consiglio di direzione. Tuttavia, qualora il presidente o il vicepresidente cessino di far parte del consiglio di direzione in un qualsiasi momento in corso di mandato, questo giunge automaticamente a termine alla stessa data. Il vicepresidente sostituisce d'ufficio il presidente nel caso in cui quest'ultimo non sia in grado di svolgere i propri compiti. Il presidente partecipa al voto.

2. Il consiglio di direzione tiene riunioni ordinarie almeno tre volte all'anno. Può convocare riunioni straordinarie su richiesta della Commissione, su richiesta di un terzo di tutti i suoi membri oppure su richiesta del presidente o del direttore esecutivo nell'esercizio delle sue funzioni.

3. Il direttore esecutivo partecipa alle deliberazioni, salvo diversa decisione del consiglio di direzione, ma non ha diritto di voto. Il consiglio di direzione può invitare, a sua discrezione, altre persone ad assistere alle proprie riunioni in veste di osservatori.

4. Su invito del presidente, i membri del consiglio consultivo industriale e scientifico possono partecipare senza diritto di voto alle riunioni del consiglio di direzione.

5. I membri del consiglio di direzione e i loro supplenti possono farsi assistere da consulenti o esperti, fatte salve le disposizioni del regolamento interno.

6. Il Centro di competenza provvede alle funzioni di segretariato del consiglio di direzione.

Articolo 15

Modalità di voto del consiglio di direzione

1. L'Unione detiene il 50% dei diritti di voto. I diritti di voto dell'Unione sono indivisibili.

2. Ogni Stato membro partecipante dispone di un voto.

3. Il consiglio di direzione delibera a maggioranza di almeno il 75% dei voti, compresi i voti dei membri assenti, in rappresentanza di almeno il 75% dei contributi finanziari complessivi al Centro di competenza. Il contributo finanziario sarà calcolato in base alle previsioni di spesa proposte dagli Stati membri di cui all'articolo 17, paragrafo 2, lettera c), e alla relazione sul valore dei contributi degli Stati membri partecipanti di cui all'articolo 22, paragrafo 5.

4. Solo i rappresentanti della Commissione e degli Stati membri partecipanti hanno diritto di voto.

5. Il presidente partecipa al voto.

SEZIONE II

DIRETTORE ESECUTIVO

Articolo 16

Nomina, destituzione o proroga del mandato del direttore esecutivo

1. Il direttore esecutivo è una persona in possesso di un'esperienza specifica e che gode di un'elevata reputazione nei settori in cui opera il Centro di competenza.

2. Il direttore esecutivo è assunto come agente temporaneo del Centro di competenza ai sensi dell'articolo 2, lettera a), del regime applicabile agli altri agenti.

3. Il consiglio di direzione nomina il direttore esecutivo scegliendolo da una rosa di candidati proposta dalla Commissione, in esito a una procedura di selezione aperta e trasparente.

4. Ai fini della conclusione del contratto del direttore esecutivo, il Centro di competenza è rappresentato dal presidente del consiglio di direzione.

5. La durata del mandato del direttore esecutivo è di quattro anni. Entro la fine di tale periodo, la Commissione esegue una valutazione che tiene conto della prestazione del direttore esecutivo e dei compiti e delle sfide futuri del Centro di competenza.

6. Agendo su proposta della Commissione, la quale tiene conto della valutazione di cui al paragrafo 5, il consiglio di direzione può prorogare il mandato del direttore esecutivo una sola volta, per non più di quattro anni.

7. Un direttore esecutivo il cui mandato sia stato prorogato non può partecipare a un'altra procedura di selezione per lo stesso posto.

8. Il direttore esecutivo è rimosso dall'incarico solo su decisione del consiglio di direzione, che agisce su proposta della Commissione.

Articolo 17

Funzioni del direttore esecutivo

1. Il direttore esecutivo è incaricato delle operazioni e della gestione quotidiana del Centro di competenza, di cui è il rappresentante legale. Il direttore esecutivo è responsabile dinanzi al consiglio di direzione e svolge le proprie funzioni in assoluta indipendenza nell'ambito delle proprie competenze.

2. Il direttore esecutivo svolge in particolare i seguenti compiti in modo indipendente:

a) attua le decisioni adottate dal consiglio di direzione;

b) sostiene il consiglio di direzione nel suo lavoro, provvede al segretariato per le sue riunioni e fornisce tutte le informazioni necessarie per l'esercizio delle sue funzioni;

c) dopo essersi consultato con il consiglio di direzione e con la Commissione, prepara il progetto di piano strategico pluriennale e il progetto di piano di lavoro annuale del Centro di competenza e li presenta per l'adozione al consiglio di direzione, specificando l'oggetto degli inviti a presentare proposte, degli inviti a manifestare interesse e dei bandi di gara necessari per attuare il piano di lavoro e le corrispondenti previsioni di spesa proposte dagli Stati membri e dalla Commissione;

d) prepara il progetto di bilancio annuale, compresa la tabella dell'organico con l'indicazione del numero di agenti temporanei per gruppo di funzioni e per grado, nonché del numero di agenti contrattuali e di esperti nazionali distaccati espressi in equivalenti a tempo pieno, e lo presenta per l'adozione al consiglio di direzione;

e) attua il piano di lavoro e riferisce al consiglio di direzione in merito;

f) prepara il progetto di relazione annuale di attività del Centro di competenza, comprensivo delle informazioni sulle spese relative;

g) garantisce l'attuazione di procedure efficaci di monitoraggio e valutazione delle prestazioni del Centro di competenza;

h) predispone un piano d'azione per dare seguito alle conclusioni delle valutazioni retrospettive e per riferire ogni due anni alla Commissione sui progressi compiuti;

i) prepara, negozia e conclude gli accordi con i centri nazionali di coordinamento;

j) è incaricato delle questioni amministrative, finanziarie e del personale, compresa l'esecuzione del bilancio del Centro di competenza, tenendo in debito conto i pareri ricevuti dalla funzione di revisione contabile nei limiti della delega conferitagli dal consiglio di direzione;

k) approva e gestisce la pubblicazione degli inviti a presentare proposte, conformemente al programma di lavoro, e gestisce le convenzioni e le decisioni di sovvenzione;

l) approva l'elenco delle azioni selezionate per il finanziamento sulla base della graduatoria stilata da un gruppo di esperti indipendenti;

m) approva e gestisce la pubblicazione dei bandi di gara, conformemente al programma di lavoro, e gestisce i contratti;

n) approva le offerte selezionate ai fini di finanziamento;

o) sottopone il progetto di bilancio e di conti annuali alla funzione di revisione contabile e, successivamente, al consiglio di direzione;

p) assicura lo svolgimento della valutazione e della gestione dei rischi;

q) firma le singole convenzioni e decisioni di sovvenzione e i singoli contratti di sovvenzione;

r) firma i contratti di appalto;

s) predispone un piano d'azione a seguito delle conclusioni delle relazioni di revisione contabile interne ed esterne e delle indagini dell'Ufficio europeo per la lotta antifrode (OLAF) e riferisce due volte l'anno sui progressi compiuti alla Commissione e periodicamente al consiglio di direzione;

t) predispone il progetto della regolamentazione finanziaria applicabile al Centro di competenza;

u) istituisce un sistema di controllo interno efficace ed efficiente e ne assicura il funzionamento; riferisce al consiglio di direzione ogni modifica sostanziale dello stesso;

v) garantisce un'efficace comunicazione con le istituzioni dell'Unione;

w) prende ogni altro provvedimento necessario per valutare i progressi realizzati dal Centro di competenza nel perseguimento della sua missione e dei suoi obiettivi enunciati agli articoli 3 e 4 del presente regolamento;

x) svolge qualsiasi altro compito affidatogli o delegatogli dal consiglio di direzione.

SEZIONE III

CONSIGLIO CONSULTIVO INDUSTRIALE E SCIENTIFICO

Articolo 18

Composizione del consiglio consultivo industriale e scientifico

1. Il consiglio consultivo industriale e scientifico è composto da un massimo di 16 membri. Il consiglio di direzione nomina i membri tra i rappresentanti degli enti della comunità delle competenze in materia di cibersicurezza.

2. I membri del consiglio consultivo industriale e scientifico possiedono competenze nella ricerca, nello sviluppo industriale, nei servizi professionali in materia di cibersicurezza o in merito alla loro diffusione. I requisiti inerenti a tali competenze sono ulteriormente specificati dal consiglio di direzione.

3. Le procedure relative alla nomina dei membri del consiglio di direzione e al funzionamento del consiglio consultivo sono specificate nel regolamento interno del Centro di competenza e sono rese pubbliche.

4. La durata del mandato dei membri del consiglio consultivo industriale e scientifico è di tre anni. Il mandato è rinnovabile.

5. Possono far parte del consiglio consultivo industriale e scientifico, e fornire il loro supporto ai lavori, rappresentanti della Commissione e dell'Agenzia europea per la sicurezza delle reti e dell'informazione.

Articolo 19

Funzionamento del consiglio consultivo industriale e scientifico

1. Il consiglio consultivo industriale e scientifico si riunisce almeno due volte l'anno.

2. Il consiglio consultivo industriale e scientifico fornisce al consiglio di direzione il proprio parere in merito all'istituzione di gruppi di lavoro su questioni specifiche

inerenti all'attività del Centro di competenza, ove necessario con il coordinamento generale di uno o più membri del consiglio consultivo industriale e scientifico.

3. Il consiglio consultivo industriale e scientifico elegge il proprio presidente.

4. Il consiglio consultivo industriale e scientifico adotta il proprio regolamento interno, che prevede anche la designazione dei rappresentanti del gruppo consultivo e la durata della loro nomina.

Articolo 20

Funzioni del consiglio consultivo industriale e scientifico

Il consiglio consultivo industriale e scientifico fornisce consulenza al Centro di competenza relativamente allo svolgimento delle sue attività e:

1) fornisce al direttore esecutivo e al consiglio di direzione consulenza strategica e il proprio contributo per la redazione del piano di lavoro e del piano strategico pluriennale entro i termini fissati dal consiglio di direzione;

2) organizza consultazioni pubbliche aperte a tutti i portatori di interessi pubblici e privati del settore della cibersicurezza, al fine di raccogliere indicazioni per la consulenza strategica di cui al paragrafo 1;

3) promuove e raccoglie informazioni sul piano di lavoro e sul piano strategico pluriennale del Centro di competenza.

CAPO III

DISPOSIZIONI FINANZIARIE

Articolo 21

Contributo finanziario dell'Unione

1. Il contributo dell'Unione al Centro di competenza a copertura delle spese amministrative e dei costi operativi comprende:

a) 1 981 668 000 EUR dal programma Europa digitale, di cui fino a 23 746 000 EUR per le spese amministrative;

b) un importo proveniente dal programma Orizzonte Europa, anche a copertura delle spese amministrative, che deve essere determinato tenendo conto del processo di pianificazione strategica da svolgersi ai sensi dell'articolo 6, paragrafo 6, del regolamento XXX [regolamento su Orizzonte Europa].

2. Il contributo massimo dell'Unione per le spese amministrative è prelevato dagli stanziamenti del bilancio generale dell'Unione assegnati al [programma Europa digitale] e al programma specifico di attuazione di Orizzonte Europa, stabilito dalla decisione XXX.

3. Il Centro di competenza attua azioni relative alla cibersicurezza del [programma Europa digitale] e del [programma Orizzonte Europa] a norma dell'articolo 62, lettera c), punto iv), del regolamento (UE, Euratom) XXX[29] [il regolamento finanziario].

[29] [aggiungere il titolo completo e il riferimento alla GU]

4. Il contributo finanziario dell'Unione non copre le attività di cui all'articolo 4, paragrafo 8, lettera b).

Articolo 22

Contributi degli Stati membri partecipanti

1. Gli Stati membri partecipanti apportano ai costi operativi e alle spese amministrative del Centro di competenza un contributo complessivo almeno pari agli importi di cui all'articolo 21, paragrafo 1, del presente regolamento.

2. Ai fini della valutazione dei contributi di cui all'articolo 23, paragrafo 1, e al paragrafo 3, lettera b), punto ii), i costi sono determinati secondo le prassi contabili abitualmente seguite dagli Stati membri interessati, le norme contabili applicabili dello Stato membro, le norme contabili internazionali e i principi internazionali di informativa finanziaria. I costi sono certificati da un revisore indipendente esterno nominato dallo Stato membro interessato. Il metodo di valutazione può essere verificato dal Centro di competenza in caso di dubbi sulla certificazione.

3. Se uno degli Stati membri partecipanti non adempie ai suoi impegni per quanto riguarda il contributo finanziario, il direttore esecutivo lo richiama per iscritto mediante notifica e fissa un termine ragionevole entro il quale ovviare all'inadempienza. Se lo Stato interessato non pone rimedio alla situazione entro il termine stabilito, il direttore esecutivo convoca una riunione del consiglio di direzione per decidere se revocare il diritto di voto allo Stato membro inadempiente o applicare altre misure fino a quando il membro non avrà adempiuto ai suoi obblighi. I diritti di voto dello Stato membro inadempiente sono sospesi finché non verrà posto rimedio all'inadempimento dei suoi impegni.

4. La Commissione può annullare, ridurre proporzionalmente o sospendere il contributo finanziario dell'Unione al Centro di competenza qualora lo Stato membro partecipante non versi i contributi di cui al paragrafo 1, li versi solo parzialmente o li versi in ritardo.

5. Gli Stati membri partecipanti riferiscono al consiglio di direzione, entro il 31 gennaio di ogni anno, in merito al valore dei contributi di cui al paragrafo 1 versati in ciascuno dei precedenti esercizi finanziari.

Articolo 23

Costi e risorse del Centro di competenza

1. Il Centro di competenza è finanziato congiuntamente dall'Unione e dagli Stati membri mediante contributi finanziari versati ratealmente e contributi corrispondenti ai costi sostenuti dai centri nazionali di coordinamento e dai beneficiari per la realizzazione delle azioni, qualora non rimborsati dal Centro di competenza.

2. Le spese amministrative del Centro di competenza non devono superare [numero] EUR e devono essere coperte da contributi finanziari divisi equamente su base annua tra l'Unione e gli Stati membri partecipanti. Qualora una parte del contributo destinato a coprire le spese amministrative non sia utilizzata, può essere resa disponibile per coprire i costi operativi del Centro di competenza.

3. I costi operativi del Centro di competenza sono coperti mediante:

   a) il contributo finanziario dell'Unione;

   b) contributi degli Stati membri partecipanti sotto forma di:

i) contributi finanziari; e

ii) se del caso, contributi in natura da parte degli Stati membri, corrispondenti ai costi sostenuti dai centri nazionali di coordinamento e dai beneficiari per la realizzazione di azioni indirette, al netto del contributo del Centro di competenza e di qualsiasi altro eventuale contributo dell'Unione a copertura degli stessi costi.

4. Le risorse del Centro di competenza iscritte a bilancio si compongono dei seguenti contributi:

a) contributi finanziari degli Stati membri partecipanti a copertura delle spese amministrative;

b) contributi finanziari degli Stati membri partecipanti a copertura dei costi operativi;

c) eventuali entrate generate dal Centro di competenza;

d) eventuali altri contributi finanziari, risorse ed entrate.

5. Gli interessi maturati dai contributi versati al Centro di competenza dagli Stati membri partecipanti sono considerati un'entrata del Centro.

6. Tutte le risorse del Centro di competenza e le sue attività sono finalizzate al conseguimento degli obiettivi fissati all'articolo 4.

7. Il Centro di competenza è proprietario di tutti gli attivi che genera o che gli sono trasferiti ai fini della realizzazione dei suoi obiettivi.

8. Le eventuali eccedenze rispetto alle spese non sono ridistribuite ai membri partecipanti del Centro di competenza, salvo in caso di scioglimento del Centro stesso.

Articolo 24

Impegni finanziari

Gli impegni finanziari del Centro di competenza non superano l'importo delle risorse finanziarie disponibili o imputate al suo bilancio dai suoi membri.

Articolo 25

Esercizio finanziario

L'esercizio finanziario ha inizio il 1° gennaio e si chiude il 31 dicembre.

Articolo 26

Formazione del bilancio

1. Ogni anno il direttore esecutivo redige un progetto di stato di previsione delle entrate e delle spese del Centro di competenza per l'esercizio finanziario successivo e lo trasmette al consiglio di direzione, corredato di un progetto di tabella dell'organico. Le entrate e le spese risultano in pareggio. Le spese del Centro di competenza comprendono le spese amministrative, infrastrutturali, di esercizio e per il personale. Le spese amministrative sono ridotte al minimo.

2. Ogni anno il consiglio di direzione elabora, sulla base del progetto di stato di previsione delle entrate e delle spese di cui al paragrafo 1, lo stato di previsione delle entrate e delle spese del Centro di competenza per l'esercizio finanziario successivo.

3. Entro il 31 gennaio di ogni anno il consiglio di direzione invia alla Commissione lo stato di previsione di cui al paragrafo 2, come parte integrante del progetto di documento unico di programmazione.

4. Sulla base di tale stato di previsione, la Commissione iscrive le stime che ritiene necessarie per quanto concerne la tabella dell'organico e l'importo del contributo a carico del bilancio generale nel progetto di bilancio dell'Unione che sottopone al Parlamento europeo e al Consiglio conformemente agli articoli 313 e 314 del TFUE.

5. Il Parlamento europeo e il Consiglio autorizzano gli stanziamenti a titolo del contributo destinato al Centro di competenza.

6. Il Parlamento europeo e il Consiglio adottano la tabella dell'organico del Centro di competenza.

7. Insieme al piano di lavoro, il consiglio di direzione adotta il bilancio del Centro. Esso diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione. Se del caso, il consiglio di direzione modifica il bilancio e il piano di lavoro del Centro di competenza per conformarli al bilancio generale dell'Unione.

Articolo 27

Rendicontazione e discarico del Centro di competenza

La rendicontazione provvisoria e definitiva e il discarico del Centro di competenza seguono le regole e il calendario del regolamento finanziario e delle sue norme finanziarie adottate conformemente all'articolo 29.

Articolo 28

Relazioni operative e finanziarie

1. Il direttore esecutivo riferisce annualmente al consiglio di direzione in merito all'espletamento delle sue funzioni conformemente al regolamento finanziario del Centro di competenza.

2. Entro due mesi dalla chiusura di ciascun esercizio finanziario, il direttore esecutivo sottopone all'approvazione del consiglio di direzione una relazione annuale di attività sui progressi compiuti dal Centro di competenza nell'anno civile precedente, in particolare in riferimento al piano di lavoro relativo a quell'anno. Tale relazione include, tra l'altro, informazioni sui seguenti aspetti:

   a) le azioni operative svolte e le spese corrispondenti;

   b) le azioni presentate, suddivise per tipologia di partecipanti, comprese le PMI, e per Stato membro;

   c) le azioni selezionate per il finanziamento, suddivise per tipologia di partecipanti, comprese le PMI, e per Stato membro nonché l'indicazione del contributo erogato dal Centro di competenza ai singoli partecipanti e alle singole azioni;

   d) i progressi ottenuti verso il raggiungimento degli obiettivi enunciati all'articolo 4 e le proposte di ulteriori azioni necessarie per conseguirli.

3. Una volta approvata dal consiglio di direzione, la relazione annuale di attività è resa pubblica.

Articolo 29

Regolamento finanziario

Il Centro di competenza adotta il proprio regolamento finanziario a norma dell'articolo 70 del regolamento XXX [nuovo regolamento finanziario].

Articolo 30

Tutela degli interessi finanziari

1. Il Centro di competenza adotta provvedimenti opportuni volti a garantire che, nella realizzazione delle azioni finanziate ai sensi del presente regolamento, gli interessi finanziari dell'Unione siano tutelati mediante l'applicazione di misure preventive contro la frode, la corruzione e ogni altra attività illecita, mediante controlli efficaci e, ove fossero rilevate irregolarità, mediante il recupero delle somme indebitamente versate e, se del caso, sanzioni effettive, proporzionate e dissuasive.

2. Il Centro di competenza accorda al personale della Commissione e alle altre persone da essa autorizzate, nonché alla Corte dei conti, l'accesso ai propri siti e locali, nonché a tutte le informazioni, anche in formato elettronico, necessarie per effettuare i controlli.

3. L'Ufficio europeo per la lotta antifrode (OLAF) può effettuare indagini, inclusi controlli e verifiche sul posto, conformemente alle disposizioni e alle procedure di cui al regolamento (Euratom, CE) n. 2185/96 del Consiglio[30] e al regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio[31], per accertare eventuali frodi, casi di corruzione o altre attività illecite lesive degli interessi finanziari dell'Unione in relazione a convenzioni di sovvenzione o a contratti finanziati, direttamente o indirettamente, conformemente al presente regolamento.

4. Fatti salvi i paragrafi 1, 2 e 3 del presente articolo, i contratti e le convenzioni di sovvenzione derivanti dall'attuazione del presente regolamento contengono disposizioni che autorizzano espressamente la Commissione, il Centro di competenza, la Corte dei conti e l'OLAF a eseguire tali controlli e indagini nei limiti delle loro rispettive competenze. Qualora l'attuazione di un'azione sia esternalizzata o subdelegata, in tutto o in parte, o richieda l'aggiudicazione di un appalto o la concessione di un sostegno finanziario a terzi, il contratto o la convenzione di sovvenzione includono l'obbligo per il contraente o il beneficiario di imporre a eventuali terze parti interessate l'accettazione esplicita di questi poteri della Commissione, del Centro di competenza, della Corte dei conti e dell'OLAF.

CAPO IV

[30] Regolamento (Euratom, CE) n. 2185/96 del Consiglio, dell'11 novembre 1996, relativo ai controlli e alle verifiche sul posto effettuati dalla Commissione ai fini della tutela degli interessi finanziari delle Comunità europee contro le frodi e altre irregolarità (GU L 292 del 15.11.1996, pag. 2).

[31] Regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, dell'11 settembre 2013, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e che abroga il regolamento (CE) n. 1073/1999 del Parlamento europeo e del Consiglio e il regolamento (Euratom) n. 1074/1999 del Consiglio (GU L 248 del 18.9.2013, pag. 1).

PERSONALE DEL CENTRO DI COMPETENZA

Articolo 31

Personale

1. Al personale del Centro di competenza si applicano lo statuto dei funzionari e il regime applicabile agli altri agenti dell'Unione europea, quale definito dal regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio[32] ("Statuto dei funzionari" e "Regime applicabile agli altri agenti"), e le norme adottate di comune accordo dalle istituzioni dell'Unione per l'applicazione dello statuto dei funzionari e del regime applicabile agli altri agenti.
2. Il consiglio di direzione esercita, nei confronti del personale del Centro di competenza, i poteri conferiti dallo statuto dei funzionari all'autorità che ha il potere di nomina e i poteri conferiti dal regime applicabile agli altri agenti all'autorità abilitata a stipulare contratti ("poteri dell'autorità che ha il potere di nomina").
3. Il consiglio di direzione adotta, a norma dell'articolo 110 dello statuto dei funzionari, una decisione basata sull'articolo 2, paragrafo 1, dello statuto dei funzionari e sull'articolo 6 del regime applicabile agli altri agenti, con cui delega al direttore esecutivo i poteri pertinenti dell'autorità che ha il potere di nomina e definisce le condizioni di sospensione di tale delega. Il direttore esecutivo è autorizzato a subdelegare tali poteri.
4. Se circostanze eccezionali lo richiedono, il consiglio di direzione può, mediante decisione, sospendere temporaneamente i poteri dell'autorità che ha il potere di nomina delegati al direttore esecutivo, nonché qualsiasi potere subdelegato da quest'ultimo. In tale caso il consiglio di direzione esercita i poteri dell'autorità che ha il potere di nomina o li delega a uno dei suoi membri o a un membro del personale del Centro di competenza che non sia il direttore esecutivo.
5. Il consiglio di direzione adotta modalità per garantire l'attuazione dello statuto dei funzionari e del regime applicabile agli altri agenti conformemente all'articolo 110 dello statuto dei funzionari.
6. Il numero degli effettivi è stabilito nella tabella dell'organico del Centro di competenza, che indica il numero di posti temporanei per gruppo di funzioni e per grado e il numero di agenti contrattuali espresso in equivalenti a tempo pieno, in linea con il bilancio annuale.
7. Il personale del Centro di competenza è costituito da personale temporaneo e a contratto.
8. Tutte le spese di personale sono a carico del Centro di competenza.

Articolo 32

Esperti nazionali distaccati e altro personale

[32] Regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio, del 29 febbraio 1968, che definisce lo statuto dei funzionari delle Comunità europee nonché il regime applicabile agli altri agenti di tali Comunità, e istituisce speciali misure applicabili temporaneamente ai funzionari della Commissione (GU L 56 del 4.3.1968, pag. 1).

1. Il Centro di competenza può avvalersi di esperti nazionali distaccati o di altro personale non alle sue dipendenze.

2. D'intesa con la Commissione, il consiglio di direzione adotta una decisione che stabilisce le disposizioni applicabili al distacco di esperti nazionali presso il Centro di competenza.

Articolo 33

Privilegi e immunità

Al Centro di competenza e al suo personale si applica il protocollo n. 7 sui privilegi e le immunità dell'Unione europea, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea.

CAPO V
DISPOSIZIONI COMUNI

Articolo 34

Norme di sicurezza

1. Alla partecipazione a tutte le azioni finanziate dal Centro di competenza si applicano le disposizioni dell'articolo 12, paragrafo 7, del regolamento (UE) n. XXX [programma Europa digitale].

2. Le seguenti norme di sicurezza specifiche si applicano ad azioni finanziate da Orizzonte Europa:

   a) ai fini dell'articolo 34, paragrafo 1 [proprietà e tutela], del regolamento (UE) n. XXX [Orizzonte Europa], qualora il piano di lavoro lo preveda, è possibile limitare la concessione di licenze non esclusive a terzi stabiliti o considerati stabiliti negli Stati membri e controllati da Stati membri e/o cittadini di Stati membri;

   b) ai fini dell'articolo 36, paragrafo 4, lettera b) [trasferimento e concessione di licenze], del regolamento (UE) n. XXX [Orizzonte Europa], il trasferimento o la concessione di una licenza a favore di un soggetto stabilito in un paese associato o nell'Unione, ma controllato da paesi terzi, possono costituire un motivo per opporsi al trasferimento di proprietà dei risultati o alla concessione di licenze esclusive sui risultati;

   c) ai fini dell'articolo 37, paragrafo 3, lettera a) [diritti di accesso] del regolamento (UE) n. XXX [Orizzonte Europa], qualora il piano di lavoro lo preveda, è possibile limitare la concessione dell'accesso ai risultati e alle conoscenze a un solo soggetto giuridico stabilito o considerato stabilito in uno Stato membro e controllato da Stati membri e/o cittadini di Stati membri.

Articolo 35

Trasparenza

1. Il Centro di competenza svolge le proprie attività con un livello elevato di trasparenza.

2. Il Centro di competenza provvede affinché il pubblico e le parti interessate dispongano di informazioni adeguate, obiettive, affidabili e facilmente accessibili, in particolare sui risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese a norma dell'articolo 41.

3. Il consiglio di direzione, su proposta del direttore esecutivo, può autorizzare le parti interessate a presenziare in qualità di osservatori allo svolgimento di alcune attività del Centro di competenza.

4. Il Centro di competenza stabilisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di trasparenza di cui ai paragrafi 1 e 2. Ai fini delle azioni finanziate da Orizzonte Europa, si terrà debitamente conto delle disposizioni di cui all'allegato III del regolamento su Orizzonte Europa.

Articolo 36

Norme di sicurezza per la protezione delle informazioni classificate e delle informazioni sensibili non classificate

1. Fatto salvo l'articolo 35, il Centro di competenza non rivela a terzi le informazioni da esso trattate o ricevute in relazione alle quali è stata presentata una richiesta motivata di trattamento riservato, integralmente o in parte.

2. I membri del consiglio di direzione, il direttore esecutivo, i membri del consiglio consultivo industriale e scientifico, gli esperti esterni che partecipano ai gruppi di lavoro *ad hoc* e il personale del Centro rispettano gli obblighi di riservatezza di cui all'articolo 339 del trattato sul funzionamento dell'Unione europea, anche dopo la cessazione delle proprie funzioni.

3. Il consiglio di direzione del Centro di competenza adotta le norme di sicurezza del Centro di competenza, a seguito dell'approvazione della Commissione, sulla base dei principi e delle regole stabilite nelle norme di sicurezza della Commissione per la protezione delle informazioni classificate UE (ICUE) e delle informazioni sensibili non classificate, comprese fra l'altro le disposizioni per il trattamento e la conservazione di tali informazioni di cui alle decisioni (UE, Euratom) 2015/443[33] e 2015/444[34] della Commissione.

4. Il Centro di competenza può adottare tutte le misure necessarie per semplificare lo scambio di informazioni utili allo svolgimento delle sue funzioni con la Commissione e gli Stati membri e con le agenzie e gli organismi dell'Unione interessati. Tutti gli accordi amministrativi stipulati a tale fine in merito alla condivisione di ICUE o, in assenza di un tale accordo, qualsiasi comunicazione eccezionale *ad hoc* di ICUE deve essere approvata dalla Commissione in via preliminare.

Articolo 37

Accesso ai documenti

[33] Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41).

[34] Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53).

1. Ai documenti detenuti dal Centro di competenza si applicano le disposizioni del regolamento (CE) n. 1049/2001.

2. Entro sei mesi dall'istituzione del Centro di competenza, il consiglio di direzione adotta disposizioni per l'attuazione del regolamento (CE) n. 1049/2001.

3. Le decisioni adottate dal Centro di competenza a norma dell'articolo 8 del regolamento (CE) n. 1049/2001 possono formare oggetto di una denuncia presentabile al Mediatore europeo a norma dell'articolo 228 del trattato sul funzionamento dell'Unione europea o di un ricorso dinanzi alla Corte di giustizia dell'Unione europea a norma dell'articolo 263 del trattato sul funzionamento dell'Unione europea.

Articolo 38

Monitoraggio, valutazione e riesame

1. Il Centro di competenza garantisce che le sue attività, comprese quelle gestite attraverso i centri nazionali di coordinamento e la rete, siano oggetto di un monitoraggio continuo e sistematico e di periodiche valutazioni. Il Centro di competenza garantisce una raccolta efficiente, efficace e tempestiva dei dati per il monitoraggio dell'attuazione e dei risultati del programma. Sono imposti obblighi di relazione proporzionati ai destinatari dei fondi dell'Unione e degli Stati membri. Gli esiti della valutazione sono resi pubblici.

2. La Commissione effettua una valutazione intermedia del Centro di competenza non appena siano disponibili informazioni sufficienti sull'attuazione del presente regolamento e comunque non oltre tre anni e mezzo dall'inizio della sua attuazione. La Commissione prepara una relazione su tale valutazione e la trasmette al Parlamento europeo e al Consiglio entro il 31 dicembre 2024. Il Centro di competenza e gli Stati membri forniscono alla Commissione le informazioni necessarie per redigere tale relazione.

3. La valutazione di cui al paragrafo 2 include un esame dei risultati conseguiti dal Centro di competenza in relazione ai suoi obiettivi, al suo mandato e alle sue funzioni. Se ritiene che sia giustificato mantenere il Centro di competenza, tenuto conto degli obiettivi, del mandato e delle funzioni di quest'ultimo, la Commissione può proporre che la durata del mandato del Centro di competenza quale indicata all'articolo 46 sia prorogata.

4. Sulla base delle conclusioni della valutazione intermedia di cui al paragrafo 2, la Commissione può procedere come previsto all'[articolo 22, paragrafo 5] o adottare qualsiasi altro provvedimento appropriato.

5. Il monitoraggio, la valutazione, la soppressione graduale e il rinnovo del contributo di Orizzonte Europa seguiranno le disposizioni di cui agli articoli 8, 45 e 47 e all'allegato III del regolamento su Orizzonte Europa e delle modalità di attuazione concordate.

6. Il monitoraggio, le rendicontazione e la valutazione in merito al contributo di Europa digitale seguiranno le disposizioni di cui agli articoli 24 e 25 del programma Europa digitale.

7. In caso di scioglimento del Centro di competenza, la Commissione esegue una valutazione finale del Centro di competenza entro sei mesi dal suo scioglimento, ma non oltre due anni dopo l'avvio della procedura di scioglimento di cui all'articolo 46

del presente regolamento. I risultati della valutazione finale sono presentati al Parlamento europeo e al Consiglio.

Articolo 39

Responsabilità del Centro di competenza

1. La responsabilità contrattuale del Centro di competenza è regolata dalla legge applicabile all'accordo, alla decisione o al contratto in causa.
2. In caso di responsabilità extracontrattuale, il Centro di competenza risarcisce, conformemente ai principi generali comuni alle leggi degli Stati membri, i danni causati dal personale nell'esercizio delle sue funzioni.
3. Tutti i pagamenti effettuati dal Centro di competenza connessi alla responsabilità di cui ai paragrafi 1 e 2, nonché i costi e le spese sostenuti in relazione ad essa, sono considerati spese del Centro di competenza e sono coperti dalle risorse del Centro.
4. Il Centro di competenza è il solo responsabile del rispetto dei propri obblighi.

Articolo 40

Competenza della Corte di giustizia dell'Unione europea e diritto applicabile

1. La Corte di giustizia dell'Unione europea è competente a pronunciarsi:
    1) in base alle clausole compromissorie contenute negli accordi, nelle decisioni o nei contratti stipulati dal Centro di competenza;
    2) sulle controversie relative al risarcimento dei danni causati dal personale del Centro di competenza nell'esercizio delle sue funzioni;
    3) sulle controversie tra il Centro di competenza e il suo personale, nei limiti e alle condizioni fissati dallo statuto dei funzionari.
2. Per tutte le questioni non contemplate dal presente regolamento o da altri atti giuridici del diritto dell'Unione, si applica il diritto dello Stato membro in cui ha sede il Centro di competenza.

Articolo 41

Responsabilità dei membri e assicurazioni

1. La responsabilità finanziaria dei membri del Centro di competenza per i debiti contratti da quest'ultimo è limitata al rispettivo contributo già versato per le spese amministrative.
2. Il Centro di competenza sottoscrive le idonee assicurazioni e le mantiene in vigore.

Articolo 42

Conflitti di interessi

Il consiglio di direzione del Centro di competenza adotta norme per la prevenzione e la gestione dei conflitti di interessi che riguardino i suoi membri, i suoi organi e il suo personale. Tali norme contengono disposizioni volte a evitare situazioni di conflitto di interessi per i rappresentanti dei membri che fanno parte del consiglio di direzione e del consiglio consultivo industriale e scientifico, ai sensi del regolamento XXX [nuovo regolamento finanziario].

Articolo 43

Protezione dei dati personali

1. Il trattamento dei dati personali da parte del Centro di competenza è soggetto al regolamento (UE) n. XXX/2018 del Parlamento europeo e del Consiglio.
2. Il consiglio di direzione adotta le misure di attuazione di cui all'articolo xx, paragrafo 3, del regolamento (UE) n. xxx/2018. Il consiglio di direzione può adottare misure aggiuntive necessarie per l'applicazione del regolamento (UE) n. xxx/2018 da parte del Centro di competenza.

Articolo 44

Sostegno da parte dello Stato membro ospitante

Tra il Centro di competenza e lo Stato membro [Belgio] in cui esso ha sede può essere concluso un accordo amministrativo concernente i privilegi e le immunità e altre agevolazioni che tale Stato membro è tenuto a concedere al Centro di competenza.

CAPO VII

DISPOSIZIONI FINALI

Articolo 45

Azioni iniziali

1. La Commissione è responsabile dell'istituzione e del funzionamento iniziale del Centro di competenza fino a quando questo non avrà la capacità operativa di eseguire il proprio bilancio. La Commissione svolge, conformemente al diritto dell'Unione, tutte le attività necessarie con il coinvolgimento degli organi competenti del Centro di competenza.
2. Ai fini del paragrafo 1, fino a quando il direttore esecutivo non assume le sue funzioni dopo essere stato nominato dal consiglio di direzione a norma dell'articolo 16, la Commissione può designare un direttore esecutivo *ad interim* ed esercitare i compiti assegnati al direttore esecutivo, il quale può essere assistito da un numero limitato di funzionari della Commissione. La Commissione può distaccare *ad interim* un numero limitato di suoi funzionari.
3. Il direttore esecutivo *ad interim* può autorizzare tutti i pagamenti coperti dagli stanziamenti previsti nel bilancio annuale del Centro di competenza, previa approvazione del consiglio di direzione, e può prendere decisioni e stipulare convenzioni, decisioni e contratti, anche relativi al personale, in seguito all'adozione della tabella dell'organico del Centro di competenza.

4. Il direttore esecutivo *ad interim*, di comune accordo con il direttore esecutivo del Centro di competenza e fatta salva l'approvazione del consiglio di direzione, stabilisce la data alla quale il Centro di competenza avrà la capacità di dare esecuzione al proprio bilancio. A partire da tale data, la Commissione si astiene dall'assumere impegni e dall'eseguire pagamenti per le attività del Centro di competenza.

Articolo 46

Durata

1. È istituito il Centro di competenza per il periodo compreso fra il 1° gennaio 2021 e il 31 dicembre 2029.
2. Al termine di questo periodo sarà avviata la procedura di scioglimento, a meno che non venga deciso altrimenti attraverso una revisione del presente regolamento. La procedura di scioglimento sarà avviata automaticamente nel caso in cui l'Unione o tutti gli Stati membri partecipanti si ritirino dal Centro di competenza.
3. Ai fini della procedura di scioglimento del Centro di competenza, il consiglio di direzione nomina uno o più liquidatori, i quali si attengono alle decisioni del consiglio di direzione.
4. Durante la procedura di scioglimento del Centro di competenza, le attività sono utilizzate per coprire le passività e le spese relative allo scioglimento. Eventuali eccedenze sono distribuite fra l'Unione e gli Stati membri partecipanti, proporzionalmente al loro contributo finanziario al Centro di competenza. Qualsiasi eccedenza a favore dell'Unione è restituita al bilancio dell'Unione.

Articolo 47

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

1.2. Settore/settori interessati nella struttura ABM/ABB

1.3. Natura della proposta/iniziativa

1.4. Obiettivi

1.5. Motivazione della proposta/iniziativa

1.6. Durata e incidenza finanziaria

1.7. Modalità di gestione previste

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

2.2. Sistema di gestione e di controllo

2.3. Misure di prevenzione delle frodi e delle irregolarità

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

3.2.2. Incidenza prevista sugli stanziamenti operativi

3.2.3. Incidenza prevista sugli stanziamenti di natura amministrativa

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

3.2.5. Partecipazione di terzi al finanziamento

3.3. Incidenza prevista sulle entrate

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Regolamento che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza

1.2. Settore/settori interessati nella struttura ABM/ABB[35]

Ricerca e innovazione

Investimenti strategici europei

1.3. Natura della proposta/iniziativa

☒La proposta/iniziativa riguarda **una nuova azione**

☐ La proposta/iniziativa riguarda **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[36]

☐ La proposta/iniziativa riguarda **la proroga di un'azione esistente**

☐ La proposta/iniziativa riguarda **un'azione riorientata verso una nuova azione**

1.4. Obiettivi

1.4.1. Obiettivi strategici pluriennali della Commissione oggetto della proposta/iniziativa

1. Un mercato unico digitale connesso

2. Un nuovo impulso all'occupazione, alla crescita e agli investimenti

1.4.2. Obiettivi specifici interessati

Obiettivi specifici

1.3 L'economia digitale può esprimere tutto il suo potenziale con l'aiuto di iniziative atte a consentire la piena crescita delle tecnologie digitali e dei dati.

2.1 L'Europa può restare tra i leader mondiali dell'economia digitale se le imprese europee riescono a crescere su scala mondiale, grazie a una forte imprenditorialità e a start-up vincenti, e se l'industria e i servizi pubblici guidano la trasformazione digitale.

2.2. La ricerca in Europa trova opportunità di investimento per possibili progressi tecnologici e iniziative faro, in particolare il programma Orizzonte 2020/Orizzonte Europa e il ricorso a partenariati pubblico-privati.

[35] ABM: activity-based management (gestione per attività); ABB: activity-based budgeting (bilancio per attività).

[36] A norma dell'articolo 54, paragrafo 2, lettera a) o b), del regolamento finanziario.

1.4.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

Il Centro di competenza, assieme alla rete e alla comunità, cercherà di conseguire i seguenti obiettivi:

1) contribuire all'attuazione della parte relativa alla cibersicurezza del programma Europa digitale, istituito dal regolamento n. XXX e, in particolare, delle azioni di cui all'articolo 6 del regolamento (UE) n. XXX [programma Europa digitale] e del programma Orizzonte Europa, istituito dal regolamento n. XXX, in particolare dalla sezione 2.2.6 dell'allegato I della decisione n. XXX relativa all'istituzione del programma specifico di attuazione di Orizzonte Europa - il programma quadro di ricerca e innovazione - e di altri programmi dell'UE [ove previsto dagli atti giuridici dell'Unione];

2) rafforzare le capacità, le conoscenze e le infrastrutture in materia di cibersicurezza al servizio delle imprese, del settore pubblico e delle comunità della ricerca;

3) contribuire a un'ampia implementazione dei prodotti e delle soluzioni più recenti in tutti i settori economici;

4) migliorare la comprensione della cibersicurezza e contribuire a ridurre i divari di competenze presenti nell'Unione in merito a tale settore;

5) contribuire al consolidamento della ricerca e dello sviluppo nel campo della cibersicurezza nell'Unione;

6) potenziare la collaborazione tra la sfera civile e quella della difesa per quanto concerne le tecnologie e le applicazioni a duplice uso;

7) potenziare le sinergie tra le dimensioni civile e di difesa della cibersicurezza;

8) contribuire a coordinare e agevolare l'attività della rete dei centri nazionali di coordinamento ("la rete") di cui all'articolo 10 e della comunità delle competenze in materia di cibersicurezza di cui all'articolo 12.

1.4.4. Indicatori di risultato e di incidenza

Precisare gli indicatori che permettono di seguire l'attuazione della proposta/iniziativa.

· Numero di infrastrutture/strumenti di cibersicurezza acquisiti congiuntamente.

· Accesso alle fasi di prova e sperimentazione per l'industria e i ricercatori europei della rete e nell'ambito del Centro. Per quanto riguarda le strutture già esistenti, aumento del numero di ore disponibili per le comunità dell'industria e della ricerca rispetto alla situazione attuale.

· Il numero delle comunità di utenti serviti e dei ricercatori che hanno accesso alle strutture di cibersicurezza europee aumenta rispetto al numero delle persone costrette a cercare tali risorse al di fuori dell'UE.

· Comincia ad aumentare la competitività dei fornitori europei, misurata in termini di quota del mercato globale (l'obiettivo è il 25% della quota di mercato entro il 2027), nonché in termini di quota dei risultati delle attività europee di R&S ottenuti dall'industria.

· Contributo alle tecnologie di prossima generazione in materia di cibersicurezza, misurato in termini di diritti d'autore, brevetti, pubblicazioni scientifiche e prodotti commerciali.

· Numero di piani formativi valutati e allineati per le competenze in materia di cibersicurezza, numero di programmi valutati di certificazione professionale nell'ambito della cibersicurezza.

· Numero di studenti, scienziati e utenti (dell'industria e delle pubbliche amministrazioni) che beneficiano di attività di formazione.

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine

Raggiungere una massa critica di investimenti nello sviluppo tecnologico e industriale della cibersicurezza e superare la frammentazione delle capacità nell'Unione.

1.5.2. Valore aggiunto dell'intervento dell'Unione europea

La cibersicurezza è una questione di interesse comune dell'Unione, come confermano le conclusioni del Consiglio di cui sopra e la portata e il carattere transfrontaliero di incidenti come quelli costituiti da *WannaCry* e *NonPetya*. La natura e l'entità dei problemi tecnologici della cibersicurezza e il coordinamento insufficiente degli sforzi all'interno e delle comunità dell'industria, del settore pubblico e della ricerca, nonché fra tali comunità, richiedono un ulteriore sostegno degli sforzi di coordinamento da parte dell'UE sia per aggregare una massa critica di risorse sia per garantire una migliore conoscenza e gestione delle risorse. Ciò è necessario se si considera il fabbisogno di risorse correlato a determinate capacità di ricerca, sviluppo e implementazione della cibersicurezza, l'esigenza di fornire accesso a competenze interdisciplinari in materia di cibersicurezza nell'ambito di discipline diverse (accesso che sovente è disponibile solo in parte a livello nazionale), la natura globale delle catene di valore industriale e l'attività dei concorrenti a livello mondiale che operano sui vari mercati.

Ciò richiede una quantità di risorse e competenze che difficilmente l'iniziativa individuale di un qualsiasi Stato membro riesce a mobilitare. Per esempio, una rete paneuropea di comunicazioni quantistiche potrebbe richiedere un investimento dell'UE dell'ordine di 900 milioni di EUR, a seconda degli investimenti effettuati dagli Stati membri (da collegare/integrare) e della misura in cui la tecnologia consentirà di riutilizzare le infrastrutture esistenti.

1.5.3. Insegnamenti tratti da esperienze analoghe

La valutazione intermedia di Orizzonte 2020 ha confermato tra l'altro la costante pertinenza del sostegno dell'UE a favore della R&S e delle sfide sociali (come "Società sicure", da cui è sostenuta la R&S in tema di cibersicurezza). Contestualmente, la valutazione ha confermato che consolidare la leadership industriale resta una sfida e che permane un divario in termini di innovazione, che vede l'UE in ritardo per quanto riguarda le innovazioni pionieristiche e creatrici di mercati.

La valutazione intermedia del meccanismo per collegare l'Europa (CEF) sembra confermare il valore aggiunto dell'intervento dell'UE al di là della R&S, sebbene la cibersicurezza nell'ambito del CEF abbia obiettivi (riguardanti la sicurezza operativa)

e una logica d'intervento in parte differenti. Nel contempo, la maggioranza dei destinatari delle sovvenzioni del CEF in materia di cibersicurezza (la comunità dei CSIRT nazionali) ha affermato di desiderare un programma di assistenza mirata nell'ambito del prossimo QFP.

La creazione nel 2016 del partenariato pubblico-privato (cPPP) sulla cibersicurezza nell'UE ha costituito un importante primo passo, che riunisce le comunità della ricerca, dell'industria e del settore pubblico per agevolare la ricerca e l'innovazione nella sicurezza informatica e che, entro i limiti del quadro finanziario 2014-2020, dovrebbe produrre risultati validi e maggiormente mirati nell'ambito della ricerca e dell'innovazione. Il cPPP ha consentito ai partner industriali di manifestare il loro impegno per quanto riguarda le spese da essi sostenute in aree definite nell'agenda strategica del partenariato per la ricerca e l'innovazione.

1.5.4. Compatibilità ed eventuale sinergia con altri strumenti pertinenti

La rete di competenza per la cibersicurezza e il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza apporteranno un ulteriore sostegno alle disposizioni regolamentari e agli operatori del settore della sicurezza informatica. Il mandato del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza integrerà gli sforzi dell'ENISA, ma ha un obiettivo diverso e richiede un insieme di competenze differente. Per quanto l'ENISA abbia un ruolo di consulenza in tema di ricerca e innovazione per la cibersicurezza nell'UE, il mandato proposto per quest'agenzia si concentra innanzitutto su altri compiti cruciali per il rafforzamento della resilienza in materia di cibersicurezza nell'Unione. Il Centro dovrebbe stimolare lo sviluppo e l'implementazione della tecnologia per la cibersicurezza e integrare l'impegno nella creazione di capacità in questo settore a livello dell'UE e nazionale.

Il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza collaborerà inoltre con la rete di competenza per la cibersicurezza al sostegno della ricerca per agevolare e accelerare i processi di standardizzazione e certificazione, in particolare quelli relativi ai sistemi di certificazione della cibersicurezza ai sensi del regolamento sulla cibersicurezza.

Il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza agirà come meccanismo di attuazione unico per due programmi dell'Unione a sostegno della cibersicurezza (Europa digitale e Orizzonte Europa), aumentandone la coerenza e le sinergie.

Questa iniziativa permette di integrare gli sforzi degli Stati membri fornendo un contributo adeguato ai responsabili delle politiche dell'istruzione, al fine di potenziare la formazione sulla cibersicurezza (per esempio mettendo a punto piani formativi in materia nei sistemi di istruzione a livello civile e militare, ma anche contribuendo all'istruzione di base sulla cibersicurezza). Permetterebbe inoltre di favorire l'allineamento e la valutazione costante dei programmi di certificazione professionale della cibersicurezza, tutte attività necessarie per contribuire a superare il divario di competenze in materia di cibersicurezza e facilitare l'accesso delle imprese e di altre comunità agli specialisti di cibersicurezza. L'allineamento dell'istruzione e delle competenze servirà a sviluppare una forza lavoro qualificata nell'UE nell'ambito della cibersicurezza, una risorsa fondamentale per le società di cibersicurezza e per altre industrie coinvolte in tale settore.

1.6. Durata e incidenza finanziaria

☒ Proposta/iniziativa di **durata limitata**

– ☒ Proposta/iniziativa in vigore a decorrere dall'1.1.2021 fino al 31.12.2029

– ☒ Incidenza finanziaria dal 2021 al 2027 per gli stanziamenti di impegno e dal 2021 al 2031 per gli stanziamenti di pagamento.

☐ Proposta/iniziativa di **durata illimitata**

– Attuazione con un periodo di avviamento dal AAAA al AAAA

– e successivo funzionamento a pieno ritmo.

1.7. Modalità di gestione previste[37]

☐ **Gestione diretta** ad opera della Commissione

– ☐ a opera dei suoi servizi, compreso il personale delle delegazioni dell'Unione;

– ☐ a opera delle agenzie esecutive

☐ **Gestione concorrente** con gli Stati membri

☒

Gestione indiretta con compiti di esecuzione del bilancio affidati:

– ☐ a paesi terzi od organismi da questi designati;

– ☐ a organizzazioni internazionali e rispettive agenzie (specificare);

– ☐ alla BEI e al Fondo europeo per gli investimenti;

– ☒ agli organismi di cui agli articoli 70 e 71 del regolamento finanziario;

– ☐ a organismi di diritto pubblico;

– ☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui presentano sufficienti garanzie finanziarie;

– ☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che presentano sufficienti garanzie finanziarie;

– ☐ alle persone incaricate di attuare azioni specifiche nel settore della PESC di cui al titolo V del TUE, che devono essere indicate nel pertinente atto di base.

– *Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".*

[37] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

L'articolo 28 contiene disposizioni dettagliate in materia di monitoraggio e relazioni.

2.2. Sistema di gestione e di controllo

2.2.1. Rischi individuati

Per attenuare i rischi connessi al funzionamento del Centro di competenza dopo la sua istituzione e ai ritardi, la Commissione assisterà il Centro di competenza durante questa fase per garantire la rapida assunzione del personale fondamentale e l'istituzione di un sistema di controllo interno efficiente e di procedure valide.

2.2.2. Informazioni riguardanti il sistema di controllo interno istituito

Il direttore esecutivo è incaricato delle operazioni e della gestione quotidiana del Centro di competenza, di cui è il rappresentante legale. Il direttore è responsabile dinanzi al consiglio di direzione, cui rende conto costantemente dell'evoluzione delle attività del Centro di competenza.

Il consiglio di direzione assume la responsabilità generale dell'orientamento strategico e dell'operato del Centro di competenza e sovrintende alle sue attività.

La regolamentazione finanziaria applicabile al Centro di competenza è adottata dal consiglio di direzione previa consultazione della Commissione. Essa si discosta dal regolamento (UE) n. 1271/2013 solo per esigenze specifiche di funzionamento del Centro di competenza e previo accordo della Commissione.

Il revisore contabile interno della Commissione esercita nei confronti del Centro di competenza le stesse competenze esercitate nei confronti della Commissione. La Corte dei conti ha il potere di revisione contabile, esercitabile sulla base di documenti e sul posto, su tutti i beneficiari di sovvenzioni, contraenti e subcontraenti cui il Centro di competenza ha concesso finanziamenti dell'Unione.

2.2.3. Stima dei costi e dei benefici dei controlli e valutazione del previsto livello di rischio di errore

Costi e benefici dei controlli

Il costo del controllo del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza si divide tra i costi della supervisione a livello di Commissione e i costi dei controlli operativi a livello dell'organismo preposto all'attuazione.

Il costo dei controlli a livello del Centro di competenza è stimato intorno all'1,19% degli stanziamenti di pagamento operativi a livello del Centro stesso.

Il costo della supervisione a livello di Commissione è stimato all'1,20% degli stanziamenti di pagamento operativi a livello del Centro di competenza.

Nell'ipotesi che le attività siano gestite interamente dalla Commissione, non coadiuvata da un'agenzia esecutiva o da un organismo preposto all'attuazione, il costo dei controlli sarebbe sensibilmente superiore e potrebbe aggirarsi intorno al 7,7% degli stanziamenti di pagamento.

I controlli previsti mirano a garantire una supervisione agevole ed efficace delle entità incaricate dell'attuazione da parte della Commissione, nonché a garantire il necessario livello di affidabilità a livello di Commissione.

I benefici dei controlli sono i seguenti:

- si evita la selezione di proposte troppo deboli o inadeguate;
- si ottimizzano la pianificazione e l'utilizzo dei fondi dell'UE, così da preservare il valore aggiunto europeo;
- si assicura la qualità delle convenzioni di sovvenzione, si evitano errori nell'individuazione delle persone giuridiche, si garantisce il calcolo corretto dei contributi dell'UE e si adottano le garanzie necessarie per un corretto funzionamento delle sovvenzioni;
- si individuano i costi inammissibili in fase di pagamento;
- si individuano errori che incidono sulla legittimità e sulla regolarità delle operazioni durante i controlli.

Livello di errore stimato

L'obiettivo è quello di mantenere il tasso di errore residuo al di sotto della soglia del 2% per l'intero programma, limitando contemporaneamente l'onere dei controlli per i beneficiari, in modo da cogliere il corretto punto di equilibrio tra l'obiettivo della legittimità e regolarità e altri obiettivi come l'attrattiva del programma, in particolare per le PMI, e il costo dei controlli.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste.

L'OLAF può eseguire indagini, compresi controlli e verifiche sul posto, in conformità delle disposizioni e delle procedure stabilite dal regolamento n. 883/2013 del Parlamento europeo e del Consiglio e dal regolamento (Euratom, CE) n. 2185/9640 del Consiglio, dell'11 novembre 1996, relativo ai controlli e alle verifiche sul posto effettuati dalla Commissione ai fini della tutela degli interessi finanziari dell'Unione contro le frodi e altre irregolarità, per accertare casi di frode, corruzione o altre attività illecite lesive degli interessi finanziari dell'Unione in relazione a sovvenzioni o contratti finanziati dal Centro di competenza.

Gli accordi, le decisioni e i contratti derivanti dall'attuazione del presente regolamento contengono disposizioni che autorizzano espressamente la Commissione, il Centro di competenza, la Corte dei conti e l'OLAF a eseguire controlli e indagini in base alle loro rispettive competenze.

Il Centro di competenza garantisce che gli interessi finanziari dei suoi membri siano adeguatamente tutelati effettuando o commissionando adeguati controlli interni ed esterni.

Il Centro di competenza aderisce all'accordo interistituzionale del 25 maggio 1999 tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione delle Comunità europee relativo alle indagini interne svolte dall'Ufficio europeo per la

lotta antifrode (OLAF). Il Centro di competenza adotta le misure necessarie per agevolare l'espletamento di indagini interne da parte dell'OLAF.

Il Centro di competenza adotterà una strategia antifrode basata su un'analisi dei rischi di frode e su considerazioni inerenti al rapporto costi-benefici. Il Centro di competenza protegge gli interessi finanziari dell'Unione mediante l'applicazione di misure preventive contro la frode, la corruzione e qualsiasi altra attività illecita, mediante controlli efficaci e, in caso di irregolarità rilevate, mediante il recupero degli importi erroneamente versati e, se del caso, mediante sanzioni amministrative e pecuniarie efficaci, proporzionate e dissuasive.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica del quadro finanziario pluriennale e nuova o nuove linee di bilancio di spesa proposte

- Nuove linee di bilancio di cui è chiesta la creazione

  Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio:

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero	Diss./Non diss.[38]	di paesi EFTA[39]	di paesi candidati[40]	di paesi terzi	ai sensi dell'articolo [21, paragrafo 2, lettera b)] del regolamento finanziario
Rubrica 1: Mercato unico, innovazione e digitale	01 02 XX XX Orizzonte Europa – Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza – Spese di sostegno 01 02 XX XX Orizzonte Europa – Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza 02 06 01 XX Programma Europa digitale – Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza – Spese di sostegno 02 06 01 XX Programma Europa digitale – Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza	Diss.	SÌ	SÌ (se specificato nel programma annuale di lavoro)	SÌ (limitatamente ad alcune parti del programma)	NO

[38] Diss. = stanziamenti dissociati / Non diss. = stanziamenti non dissociati.

[39] EFTA: Associazione europea di libero scambio.

[40] Paesi candidati e, se del caso, potenziali candidati dei Balcani occidentali.

- Il contributo a tali linee di bilancio è atteso dalle seguenti voci:

Mio EUR (al terzo decimale)

Linea di bilancio	Anno 2021	Anno 2022	Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027	**Totale**
01 01 01 01 Spese relative ad agenti temporanei o funzionari nell'ambito della ricerca – Orizzonte Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Personale esterno incaricato dell'attuazione dei programmi di ricerca – Orizzonte Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Altre spese di gestione per la ricerca – Orizzonte Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Sfide globali e competitività industriale	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Supporto amministrativo – Programma Europa digitale	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Cibersicurezza – Programma Europa digitale	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1.957,922**
Spese totali	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1.981,668**

Nel corso del processo legislativo e, in ogni caso, prima che venga raggiunto un accordo politico, la Commissione proporrà il contributo proveniente dalla dotazione finanziaria del polo tematico "Società inclusiva e sicura" del pilastro II, "Sfide globali e competitività industriale" di Orizzonte Europa (una dotazione complessiva di 2 800 000 000 EUR) di cui all'articolo 21, paragrafo 1, lettera b). La proposta si baserà sull'esito del processo di pianificazione strategica definito all'articolo 6, paragrafo 6, del regolamento XXX [programma quadro di Orizzonte Europa].

Gli importi di cui sopra non includono il contributo degli Stati membri ai costi operativi e alle spese amministrative del Centro di competenza, commisurato al contributo finanziario dell'Unione.

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	**1**	Mercato unico, innovazione e digitale

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Post 2027***	**TOTALE**
Titolo 1 (Spese per il personale)	Impegni = pagamenti	1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Titolo 2 (Infrastrutture e spese operative)	Impegni = pagamenti	2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Titolo 3 (spese operative)	Impegni	3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1.957,922**
	Pagamenti	4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1.061,715	**1.957,922**
TOTALE degli stanziamenti per la dotazione dei programmi[42]	Impegni	= 1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1.981,668**
	Pagamenti	= 1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1.061,715**	**1.981,668**

41 Gli stanziamenti per il personale sono contabilizzati solo per sei mesi nel 2021

42 Il totale degli stanziamenti stabiliti riguarda esclusivamente le risorse finanziarie dell'UE destinate alla cibersicurezza nell'ambito di Europa digitale. Nel corso del processo legislativo e, in ogni caso, prima che venga raggiunto un accordo politico, la Commissione proporrà il contributo proveniente dalla dotazione finanziaria del polo tematico "Società inclusiva e sicura" del pilastro II, "Sfide globali e competitività industriale" di Orizzonte Europa (una dotazione complessiva di 2 800 000 000 EUR) di cui all'articolo 5, paragrafo 1, lettera b). La proposta si baserà sull'esito del processo di pianificazione strategica definito all'articolo 6, paragrafo 6, del regolamento XXX [programma quadro di Orizzonte Europa].

Rubrica del quadro finanziario pluriennale	7	"Spese amministrative"

Mio EUR (al terzo decimale)

		2021	2022	2023	2024	2025	2026	2027	*Post 2027*	TOTALE
Risorse umane		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Altre spese amministrative		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
TOTALE degli stanziamenti per la RUBRICA 7 del quadro finanziario pluriennale	(Totale impegni = totale pagamenti)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

Mio EUR (al terzo decimale)

		2021	2022	2023	2024	2025	2026	2027	*Post 2027*	TOTALE
TOTALE degli stanziamenti per tutte le RUBRICHE del quadro finanziario pluriennale	Impegni	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2.005,637**
	Pagamenti	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1.061,715**	**2.005,637**

3.2.2. Sintesi dell'incidenza prevista sugli stanziamenti di natura amministrativa

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti di natura amministrativa.

– ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti di natura amministrativa, come spiegato di seguito:

Mio EUR (al terzo decimale)

Anni	2021	2022	2023	2024	2025	2026	2027	TOTALE
RUBRICA 7 del quadro finanziario pluriennale								
Risorse umane	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Altre spese amministrative	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Totale parziale della RUBRICA 7 del quadro finanziario pluriennale	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**

Esclusa la RUBRICA 7[43] del quadro finanziario pluriennale								
Risorse umane								
Altre spese di natura amministrativa	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Totale parziale esclusa la RUBRICA 7 del quadro finanziario pluriennale	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**

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

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese di natura amministrativa è coperto dagli stanziamenti della DG già assegnati alla gestione dell'azione e/o riassegnati all'interno della stessa DG, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese di natura amministrativa al di fuori della rubrica 7 corrisponde agli importi coperti dal contributo finanziario dell'Unione proveniente dal programma Europa digitale.

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese di natura amministrativa al di fuori della rubrica 7 verrà maggiorato degli importi coperti dal contributo finanziario dell'Unione proveniente dal programma Orizzonte Europa una volta che, nel corso del processo legislativo (e, in ogni caso, prima che venga raggiunto un accordo politico), sarà stato proposto dalla Commissione il contributo proveniente dalla dotazione finanziaria del polo tematico "Società inclusiva e

[43] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

sicura" del pilastro II, "Sfide globali e competitività industriale", di Orizzonte Europa (una dotazione complessiva di 2 800 000 000 EUR), di cui all'articolo 21, paragrafo 1, lettera b).

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese di natura amministrativa al di fuori della rubrica 7 non include il contributo degli Stati membri alle spese amministrative del Centro di competenza, commisurato al contributo finanziario dell'Unione.

3.2.2.1. Fabbisogno previsto di risorse umane nella Commissione

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

– ■ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in equivalenti a tempo pieno

Anni		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Posti della tabella dell'organico (funzionari e agenti temporanei)								
In sede e negli uffici di rappresentanza della Commissione		20	21	21	21	21	21	22
Nelle delegazioni								
Ricerca								
• Personale esterno (in equivalenti a tempo pieno: ETP) - AC, AL, END, INT e JPD [44] Rubrica 7								
Finanziato dalla RUBRICA 7 del quadro finanziario pluriennale	- in sede	3	3	3	3	3	3	3
	- nelle delegazioni							
Finanziato dalla dotazione del programma [45]	- in sede							
	- nelle delegazioni							
Ricerca								
Altro (specificare)								
TOTALE		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	Coordinamento, monitoraggio e direzione dei compiti affidati al Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, compresi i costi di sostegno e di coordinamento. Sviluppo e coordinamento delle politiche nel campo della cibersicurezza in relazione ai compiti affidati al Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, per esempio in merito alla definizione delle priorità per la ricerca e la politica industriale, alla cooperazione generale tra gli Stati membri e gli operatori economici, alla coerenza rispetto al futuro quadro di certificazione della cibersicurezza dell'UE, all'operato in termini di responsabilità e all'obbligo di diligenza o al coordinamento con le politiche in materia di calcolo ad alte prestazioni, intelligenza artificiale e competenze digitali. .
Personale esterno	Coordinamento, monitoraggio e direzione dei compiti affidati al Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, compresi i costi di

[44] AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale; JPD = giovane professionista in delegazione.

[45] Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

	sostegno e di coordinamento. Sviluppo e coordinamento delle politiche nel campo della cibersicurezza in relazione ai compiti affidati al Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, per esempio in merito alla definizione delle priorità per la ricerca e la politica industriale, alla cooperazione generale tra gli Stati membri e gli operatori economici, alla coerenza rispetto al futuro quadro di certificazione della cibersicurezza dell'UE, all'operato in termini di responsabilità e all'obbligo di diligenza o al coordinamento con le politiche in materia di calcolo ad alte prestazioni, intelligenza artificiale e competenze digitali. .

3.2.2.2. Fabbisogno previsto di risorse umane nel Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza

	2021	2022	2023	2024	2025	2026	2027
Funzionari della Commissione							
Di cui AD							
Di cui AST							
Di cui AST/SC							
Agenti temporanei							
Di cui AD	10	11	13	13	13	13	13
Di cui AST							
Di cui AST/SC							
Agenti contrattuali	26	32	39	39	39	39	39
END	1	1	1	1	1	1	1
Totale	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	Attuazione operativa dei compiti affidati al Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, ai sensi dell'articolo 4 del presente regolamento, compresi i costi di sostegno e di coordinamento.
Personale esterno	Attuazione operativa dei compiti affidati al Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, ai sensi dell'articolo 4 del presente regolamento, compresi i costi di sostegno e di coordinamento.

Il fabbisogno di risorse umane previsto e sopra indicato nel Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza corrisponde al fabbisogno previsto per attuare il contributo finanziario dell'Unione nell'ambito di Europa digitale.

Il fabbisogno di risorse umane previsto e sopra indicato nel Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza verrà aumentato del fabbisogno previsto per attuare il contributo finanziario dell'Unione nell'ambito di Orizzonte Europa una volta che, nel corso del processo legislativo (e, in ogni caso, prima che venga raggiunto un accordo politico), sarà stato proposto dalla Commissione il contributo proveniente dalla dotazione finanziaria del polo tematico "Società inclusiva e sicura" del pilastro II, "Sfide globali e competitività industriale", di Orizzonte Europa (una dotazione complessiva di 2 800 000 000 EUR), di cui all'articolo 21, paragrafo 1, lettera b).

3.2.2.3. Tabella dell'organico del Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza

Gruppo di funzioni e grado	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
Totale AD	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							
Totale AST							
AST/SC 6							
AST/SC 5							
AST/SC 4							

AST/SC 3							
AST/SC 2							
AST/SC 1							
Totale AST/SC							
TOTALE COMPLESSIVO	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Incidenza stimata sul personale (aggiuntivo) – personale esterno del Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza

Agenti contrattuali	2021	2022	2023	2024	2025	2026	2027
Gruppo di funzioni IV	20	22	29	29	29	29	29
Gruppo di funzioni III	2	4	4	4	4	4	4
Gruppo di funzioni II	4	6	6	6	6	6	6
Gruppo di funzioni I							
Totale	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Al fine di garantire la neutralità degli effettivi, il personale aggiuntivo del Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza sarà parzialmente compensato dalla riduzione del numero di funzionari e membri del personale esterno (con riferimento alla tabella dell'organico e al personale esterno attualmente in servizio) nei servizi pertinenti della Commissione.
Il numero di effettivi del Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza di cui ai punti da 3.2.2.2 a 3.2.2.4 sarà compensato come segue[46]:

TOTALE	2021	2022	2023	2024	2025	2026	2027
Funzionari della Commissione	5	5	6	6	6	6	6
Agenti temporanei							
Agenti contrattuali	14	17	20	20	20	20	20
END							
Totale ETP	19	22	26	26	26	26	26
Effettivi	19	22	26	26	26	26	26

[46] In base all'importo finale del bilancio, la cui esecuzione sarà delegata al Centro di competenza.

La compensazione delle risorse umane nel Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza sarà commisurata alla quota del contributo finanziario dell'Unione, ossia il 50%.

La compensazione di cui sopra riguarda il fabbisogno previsto di risorse umane nel Centro di competenza industriale, tecnologica e di ricerca sulla cibersicurezza per attuare il contributo finanziario dell'Unione nell'ambito di Europa digitale.

La compensazione di cui sopra verrà aumentata dal fabbisogno previsto per attuare il contributo finanziario dell'Unione nell'ambito di Orizzonte Europa una volta che, nel corso del processo legislativo (e, in ogni caso, prima che venga raggiunto un accordo politico), sarà stato proposto dalla Commissione il contributo proveniente dalla dotazione finanziaria del polo tematico "Società inclusiva e sicura" del pilastro II, "Sfide globali e competitività industriale", di Orizzonte Europa (una dotazione complessiva di 2 800 000 000 EUR), di cui all'articolo 21, paragrafo 1, lettera b).

3.2.3. Partecipazione di terzi al finanziamento

La proposta/iniziativa:

– ☐ non prevede cofinanziamenti da terzi.

– ☒ prevede il cofinanziamento da terzi[47] indicato di seguito:

Stanziamenti in Mio EUR (al terzo decimale)

Anni	2021	2022	2023	2024	2025	2026	2027	TOTALE
Stati membri – contributo alle spese per il personale	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Stati membri – contributo alle infrastrutture e alle spese operative	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Stati membri – contributo alle spese operative	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1.957,922**
TOTALE degli stanziamenti cofinanziati	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1.981,668**

Il contributo di terzi di cui sopra si riferisce esclusivamente al cofinanziamento commisurato alle risorse finanziarie dell'UE destinate alla cibersicurezza nell'ambito di Europa digitale. Il contributo di terzi di cui sopra verrà aumentato una volta che, nel corso del processo legislativo (e, in ogni caso, prima che venga raggiunto un accordo politico), sarà stato proposto dalla Commissione il contributo finanziario proveniente dalla dotazione finanziaria del polo tematico "Società inclusiva e sicura" del pilastro II, "Sfide globali e competitività industriale", di Orizzonte Europa (una dotazione complessiva di 2 800 000 000 EUR), di cui all'articolo 21, paragrafo 1, lettera b). La proposta si baserà sull'esito del processo di pianificazione strategica definito all'articolo 6, paragrafo 6, del regolamento XXX [programma quadro di Orizzonte Europa].

3.3. Incidenza prevista sulle entrate

– ☒ La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

– ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

☐ sulle risorse proprie

☐ su altre entrate

indicare se le entrate sono destinate a linee di spesa specifiche ☐

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Incidenza della proposta/iniziativa[48]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Articolo …….							

[47] Contributo in natura stimato degli Stati membri

[48] Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 20% per spese di riscossione.

Per quanto riguarda le entrate con destinazione specifica, precisare la linea o le linee di spesa interessate.

Altre osservazioni (ad esempio formula/metodo per calcolare l'incidenza sulle entrate o altre informazioni).