Consiglio dell'Unione europea

Bruxelles, 13 settembre 2018
(OR. en)

12104/18
ADD 5

Fascicolo interistituzionale: 2018/0328 (COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	12 settembre 2018
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	SWD(2018) 404 final
Oggetto:	DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE SINTESI DELLA VALUTAZIONE D'IMPATTO che accompagna il documento 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

Si trasmette in allegato, per le delegazioni, il documento SWD(2018) 404 final.

All.: SWD(2018) 404 final

COMMISSIONE
EUROPEA

Bruxelles, 12.9.2018
SWD(2018) 404 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA VALUTAZIONE D'IMPATTO

che accompagna il documento

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

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

Scheda di sintesi

Valutazione d'impatto su: proposta di istituzione della rete di centri di competenza e del Centro europeo di ricerca e di competenza sulla cibersicurezza

A. Necessità di intervenire

Per quale motivo? Qual è il problema da affrontare?

Attualmente l'UE non possiede ancora capacità tecnologiche e industriali sufficienti per salvaguardare la propria economia e le infrastrutture critiche in modo autonomo e per acquisire un ruolo di leadership mondiale nel campo della cibersicurezza. L'obiettivo della presente iniziativa è contribuire ad affrontare i seguenti problemi, e i relativi fattori scatenanti, che concorrono a questa situazione:

problema 1: il livello insufficiente di coordinamento e cooperazione strategica e sostenibile tra industrie, comunità della ricerca sulla cibersicurezza e governi per proteggere l'economia, la società e la democrazia con soluzioni europee all'avanguardia in materia di sicurezza informatica;

problema 2: investimenti su scala ridotta e accesso limitato alle conoscenze, alle competenze e alle strutture di cibersicurezza europee;

problema 3: in Europa sono pochi i risultati della ricerca e dell'innovazione in materia di sicurezza informatica che si sono tradotti in soluzioni commercializzabili e ampiamente diffuse in tutti i settori economici.

Questi problemi presentano alcuni fattori scatenanti di fondo, tra cui il livello insufficiente di fiducia tra gli operatori del mercato della cibersicurezza, i limiti intrinseci dei meccanismi esistenti di cooperazione e di aggregazione dei fondi, la mancanza di un quadro per l'appalto congiunto di infrastrutture costose e prodotti/soluzioni nel settore della cibersicurezza, nonché il potenziale inutilizzato dei meccanismi a monte e a valle del mercato.

Qual è l'obiettivo dell'iniziativa?

L'iniziativa mira a fare sì che l'UE mantenga e sviluppi le capacità essenziali (tecnologiche e industriali) per tutelare autonomamente la propria economia, la propria società e la propria democrazia digitali e che gli Stati membri traggano vantaggio dalle soluzioni in materia di sicurezza informatica e dalle capacità di ciberdifesa più avanzate. L'iniziativa mira altresì ad aumentare la competitività globale delle società di cibersicurezza dell'UE e a fare in modo che le industrie europee di diversi settori accedano alle capacità e alle risorse per trasformare la cibersicurezza in un vantaggio competitivo per loro. Questi obiettivi dovrebbero essere conseguiti sviluppando meccanismi efficaci per la cooperazione strategica a lungo termine di tutti gli attori pertinenti (autorità pubbliche, industrie, comunità della ricerca nell'ambito civile e in quello della difesa), condividendo conoscenze e risorse per mettere a disposizione capacità e infrastrutture all'avanguardia, stimolando un ampio utilizzo di soluzioni e prodotti europei in materia di sicurezza informatica in tutti i settori economici e in quello pubblico, sostenendo le start-up e le PMI nel campo della cibersicurezza e contribuendo a superare il divario di competenze in materia.

Qual è il valore aggiunto dell'intervento a livello dell'UE?

L'iniziativa conferirebbe un valore aggiunto agli sforzi attuali a livello nazionale contribuendo alla creazione di un ecosistema europeo dell'industria e della ricerca nel settore della cibersicurezza che concorrerebbe a migliorare la cooperazione tra le parti interessate pertinenti (fra cui i comparti deputati alla cibersicurezza dei settori civile e della difesa), per utilizzare al meglio le risorse e le competenze disponibili in tutta Europa nel campo della cibersicurezza. Sarebbe opportuno che l'UE e gli Stati membri si dessero una prospettiva strategica attiva di lungo respiro per quanto concerne la politica industriale in materia di cibersicurezza, che si spingesse al di là dell'ambito della ricerca e dello sviluppo. Una tale impostazione contribuirebbe non solo all'individuazione di soluzioni innovative alle sfide poste dalla cibersicurezza nel settore pubblico e in quello privato, ma anche all'adeguata diffusione di queste soluzioni. In questo modo si consentirebbe alle comunità della ricerca e dell'industria e alle autorità pubbliche di accedere a capacità essenziali quali le strutture di prova e sperimentazione, che sono spesso fuori della portata dei singoli Stati membri a causa dell'insufficienza di risorse finanziarie ed umane. Permettendo ai migliori talenti di partecipare a progetti europei su vasta scala, che possano costituire per loro interessanti sfide professionali, si contribuirebbe inoltre a superare il divario di competenze e ad evitare la fuga di cervelli. Tutti gli aspetti sopra indicati sono altresì ritenuti necessari affinché l'Europa venga riconosciuta a livello mondiale tra i

leader nel campo della sicurezza informatica.

B. Soluzioni

Quali opzioni strategiche legislative e di altro tipo sono state prese in considerazione? Ne è stata prescelta una? Per quale motivo?

Sono state prese in considerazione alcune opzioni strategiche, sia legislative sia non legislative. Le opzioni seguenti sono state selezionate per un esame approfondito:

1. 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 programma Orizzonte Europa;
2. **opzione 1:** rete di competenza per la cibersicurezza con un Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, cui è conferito il potere di perseguire l'attuazione di misure a supporto delle tecnologie industriali e nell'ambito della ricerca e dell'innovazione;
3. **opzione 2:** rete di competenza per la cibersicurezza con un Centro europeo di ricerca e di competenza in materia, operativa solo nell'ambito della ricerca e dell'innovazione.

Nella fase iniziale sono state scartate le seguenti opzioni: 1) l'assenza di qualsiasi intervento; 2) la sola istituzione di una rete costituita dai centri di competenza esistenti e 3) il ricorso ad un'agenzia esistente (ENISA, REA o INEA).

Considerando l'impegno generale già assunto dalla Commissione per la presente iniziativa e l'importante ruolo che devono svolgere gli Stati membri, da un'analisi dettagliata risulta che la principale distinzione tra le due opzioni strategiche risiede nel loro ambito di applicazione, che si rispecchia nella loro base giuridica: un ente fondato esclusivamente sull'articolo 187 del TFUE (opzione 2) limiterebbe la portata dell'iniziativa alla sfera della ricerca e dell'innovazione e presupporrebbe di norma un contributo finanziario da parte di soggetti privati. D'altra parte, un ente fondato su una doppia base giuridica, costituita dagli articoli 187 e 173 del TFUE (opzione 1), comporterebbe un mandato più ampio comprendente anche, fra l'altro, l'implementazione delle tecnologie e il sostegno all'industria, nonché la realizzazione di sinergie più forti con la ciberdifesa. Ciò conferirebbe agli Stati membri un ruolo più significativo, sia nell'ambito della governance che in qualità di potenziali acquirenti di tecnologia per la cibersicurezza.

L'analisi ha dimostrato 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. Fra i principali argomenti a favore di questa opzione si annoverano: la flessibilità per consentire l'adozione di diversi modelli di cooperazione con la comunità e la rete di centri di competenza per ottimizzare l'impiego delle conoscenze e delle risorse esistenti; la possibilità di strutturare la cooperazione dei portatori di interessi pubblici e privati di tutti i settori pertinenti, tra cui la difesa; 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. Infine, l'opzione 1 permette altresì di aumentare la coerenza fungendo da meccanismo di attuazione per i finanziamenti legati alla cibersicurezza provenienti dal programma Europa digitale e da Orizzonte Europa, nonché di potenziare le sinergie tra le dimensioni civile e di difesa della sicurezza informatica in relazione al Fondo europeo per la difesa.

Chi sono i sostenitori delle varie opzioni?

In base all'esito della consultazione e alle procedure di raccolta delle prove, è evidente che sia la comunità dell'industria che quella della ricerca chiedono di poter disporre di un meccanismo che permetta all'UE di avere una politica industriale coerente in materia di cibersicurezza che si spinga al di là delle attività di ricerca e sviluppo, condizione necessaria affinché l'Europa acquisisca un ruolo di leadership mondiale nel campo della cibersicurezza. Contestualmente, i portatori di interessi hanno evidenziato che la chiave del successo consisterà in un ruolo ben definito per il Centro di competenza nel sostenere e agevolare l'impegno della rete e delle comunità pertinenti, oltre ad un approccio inclusivo e collaborativo alla rete per evitare una nuova compartimentazione. Inoltre, poiché la cibersicurezza è un ambiente in rapida evoluzione, la struttura dovrebbe essere flessibile per poter essere adeguata facilmente. Nel corso dell'intero processo, gli Stati membri hanno

sottolineato l'esigenza di adottare un approccio inclusivo nei confronti di tutti gli Stati membri e dei loro centri di eccellenza e competenza e di prestare particolare attenzione alla complementarità delle iniziative. Nello specifico, per quanto riguarda il Centro, gli Stati membri hanno evidenziato l'importanza del suo ruolo di coordinamento a supporto della rete. Pertanto, qualsiasi iniziativa della Commissione dovrà trovare il giusto equilibrio nelle strutture di governance e di attuazione e riflettere tale equilibrio in queste strutture per garantire un coordinamento europeo efficace, che tenga anche conto degli sviluppi a livello nazionale.

C. Impatto dell'opzione prescelta

Quali sono i vantaggi dell'opzione prescelta (o in mancanza di quest'ultima, delle opzioni principali)?

L'opzione prescelta 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, offrendo soluzioni e prodotti più sicuri e dotandosene. In particolare, ciò è pertinente per la protezione dell'accesso a servizi essenziali (per esempio trasporti, servizi sanitari, bancari e finanziari). Inoltre avrebbe un impatto positivo per la competitività dell'UE e le PMI, in quanto presuppone la creazione di un meccanismo in grado di sviluppare le capacità industriali degli Stati membri e dell'Unione in materia di cibersicurezza e di tradurre efficacemente l'eccellenza scientifica europea in soluzioni commercializzabili che si potrebbero diffondere in tutti i settori economici. Questa opzione permette di mettere in comune risorse per investire nelle capacità necessarie a livello di Stati membri e sviluppare risorse europee comuni, realizzando nel contempo economie di scala. Ciò comporterà probabilmente un aumento dell'accesso a tali strutture per le PMI, le industrie e i ricercatori, stimolando così l'innovazione e abbreviando i processi di sviluppo, oltre a tagliare i costi per alcune imprese sul versante della domanda e ad aiutarle a trasformare la cibersicurezza in un vantaggio competitivo. L'opzione permette di sfruttare le opportunità di mercato dei prodotti a duplice uso, consentendo alle comunità nell'ambito civile e in quello della difesa di collaborare per far fronte a sfide condivise, e probabilmente conferirà anche un valore aggiunto agli sforzi nazionali volti a superare il divario di competenze in materia di cibersicurezza. A livello dell'UE, questa opzione permette inoltre di aumentare la coerenza e le sinergie tra diversi meccanismi di finanziamento.

Un effetto positivo indiretto sull'ambiente si potrebbe ottenere sviluppando soluzioni specifiche in materia di sicurezza informatica per settori con un impatto ambientale potenzialmente enorme (per esempio quello delle centrali nucleari), contribuendo a prevenire conseguenze potenzialmente devastanti di attacchi alla sicurezza informatica nei confronti di questo tipo di infrastrutture.

Quali sono i costi dell'opzione prescelta (o in mancanza di quest'ultima, delle opzioni principali)?

I costi connessi all'opzione prescelta riguardano principalmente il funzionamento del Centro di competenza e dei centri nazionali di coordinamento. I costi connessi all'attuazione di diversi programmi di finanziamento (Europa digitale e Orizzonte Europa) sono soggetti a valutazioni d'impatto distinte.

Quale sarà l'incidenza su aziende, PMI e microimprese?

Dei gruppi di portatori di interessi maggiormente interessati faranno parte aziende europee sia sul versante della domanda che su quello dell'offerta, tra cui PMI e microimprese operanti nel campo della cibersicurezza. Pur non imponendo obblighi normativi, l'istituzione del Centro di competenza e della rete offrirà opportunità in termini di riduzione dei costi per la progettazione di nuovi prodotti e aiuterà tali aziende ad accedere più facilmente alla comunità degli investitori e ad attrarre i finanziamenti necessari per realizzare soluzioni commercializzabili. Nel caso delle PMI e delle microimprese, l'accesso a strutture di prova e sperimentazione finanziate con fondi pubblici è ancora più importante, in quanto le imprese di tale tipo non hanno risorse per acquistare o reperire al di fuori del proprio mercato (spesso anche al di fuori dell'UE) le infrastrutture necessarie. Si spera inoltre che questa iniziativa apra nuovi mercati alle PMI e alle microimprese europee attive nel campo della cibersicurezza. Inoltre, il meccanismo scelto garantirà il coordinamento tra la ricerca e l'industria, orientando pertanto gli sforzi della prima verso le esigenze concrete della seconda. La messa a disposizione di competenze e strumenti di punta nel settore della cibersicurezza aiuterà indirettamente gli operatori economici a conformarsi alla direttiva NIS.

L'impatto sui bilanci e sulle amministrazioni nazionali sarà significativo?

L'iniziativa consentirà agli Stati membri di coordinare gli investimenti nelle infrastrutture di cibersicurezza necessarie a livello nazionale ed europeo e il meccanismo permetterà di aggregare risorse per infrastrutture e strumenti che altrimenti sarebbero più costosi o inaccessibili per i singoli Stati membri. Un approccio simile consentirebbe una razionalizzazione e la realizzazione di economie di scala. Il contributo finanziario degli Stati

membri destinato al Centro di competenza e alle azioni pertinenti dovrebbe essere commisurato al contributo dell'Unione.

Sono previsti altri impatti significativi?

Sì, l'iniziativa ha un chiaro impatto positivo, in quanto aumenterà, probabilmente in misura considerevole, la capacità degli Stati membri di salvaguardare in modo autonomo le proprie economie, proteggendo tra l'altro i settori critici, aumentando la competitività delle imprese europee nel campo della cibersicurezza e le industrie di diversi settori, che potranno salvaguardare adeguatamente le risorse di cui dispongono e progettare prodotti sicuri e innovativi, riducendo nel contempo i costi di ricerca e sviluppo legati alla sicurezza. In ultima analisi, questa iniziativa dovrebbe permettere all'UE di acquisire un ruolo di leadership nel campo delle tecnologie digitali e di cibersicurezza di prossima generazione.

D. Tappe successive

Quando saranno riesaminate le misure proposte?

Lo strumento giuridico comprenderà una clausola esplicita che prevederà il monitoraggio degli indicatori chiave di prestazione (IPC) e una clausola di valutazione e riesame, in virtù della quale la Commissione europea condurrà una valutazione intermedia al fine di quantificare l'impatto dello strumento e il suo valore aggiunto. Successivamente la Commissione riferirà al Parlamento europeo e al Consiglio in merito. In seguito a tale valutazione, la Commissione potrà proporre un riesame e una proroga del mandato del Centro di competenza e della rete.