Consiglio dell'Unione europea

Bruxelles, 6 dicembre 2024
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
Destinatario:	Delegazioni
Oggetto:	Conclusioni del Consiglio sull'ENISA

Si allegano per le delegazioni le conclusioni del Consiglio sull'ENISA approvate dal Consiglio nella sessione del 6 dicembre 2024.

ALLEGATO

Progetto di conclusioni del Consiglio sull'ENISA

IL CONSIGLIO DELL'UNIONE EUROPEA

1. SOTTOLINEA che le sfide derivanti dal ciberspazio globale non sono mai state così complesse, diversificate e gravi come ora, a causa della sofisticazione delle minacce informatiche emergenti, del contesto di sicurezza in costante evoluzione e delle attuali tensioni geopolitiche. Pertanto, l'UE e i suoi Stati membri dovrebbero proseguire gli sforzi per diventare più resilienti al fine di individuare e affrontare efficacemente le minacce e le sfide attuali ed emergenti. EVIDENZIA che i lavori per un maggiore livello di ciberresilienza dovrebbero essere portati avanti seguendo un approccio che coinvolga tutta la società. METTE IN RILIEVO che, nei prossimi anni, l'UE e i suoi Stati membri dovrebbero concentrarsi sull'effettiva attuazione delle iniziative legislative e non legislative che sostengono tutte le azioni intraprese finora a tale riguardo e vi contribuiscono.

2. RICORDANDO che la sicurezza nazionale rimane di responsabilità esclusiva di ciascuno Stato membro, RICONOSCE l'immenso lavoro che l'UE e gli Stati membri hanno realizzato insieme negli ultimi anni per mettere a punto l'assetto istituzionale e le forme di collaborazione necessari a livello sia nazionale che dell'UE nel settore del ciberspazio. ACCOGLIE CON FAVORE le varie iniziative legislative e non legislative che hanno fornito all'UE e agli Stati membri un quadro rigoroso e solido in questo settore, aumentando nel complesso la ciberresilienza dell'Unione. Tale quadro si è evoluto per includere vari aspetti del settore del ciberspazio, quali la sicurezza, la diplomazia, l'attività di contrasto e la difesa. OSSERVA che un gran numero di attori, tra cui le autorità per la cibersicurezza degli Stati membri, il gruppo di cooperazione NIS, la rete CSIRT, la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), la rete dei centri nazionali di coordinamento, il gruppo europeo per la certificazione della cibersicurezza (ECCG), la Commissione, il servizio europeo per l'azione esterna (SEAE), l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), il Centro europeo di competenza per la cibersicurezza (ECCC), il CERT-UE, l'Agenzia europea per la difesa (AED) e il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, fanno parte dell'ecosistema della cibersicurezza dell'UE e che ognuno di questi attori dà il proprio contributo all'attuazione del quadro in materia di cibersicurezza dell'UE.

3. RICONOSCE che negli ultimi vent'anni l'ENISA si è rivelata un'entità essenziale nell'ecosistema europeo della cibersicurezza, svolgendo un ruolo cruciale nel sostenere attivamente gli Stati membri e le istituzioni, gli organi e gli organismi dell'UE assistendoli nell'attuazione e nello sviluppo delle politiche in materia di cibersicurezza, nello sviluppo di capacità e nella preparazione, come pure nella cooperazione e nella promozione della sensibilizzazione e della certificazione in materia di cibersicurezza.

RACCOMANDAZIONI DI POLITICA GENERALE

4. INVITA la Commissione a cogliere l'opportunità della **valutazione del regolamento sulla cibersicurezza** per esaminare in che modo tale strumento possa contribuire alla semplificazione del complesso ecosistema della cibersicurezza, migliorando in tal modo l'efficacia e l'uso efficiente delle risorse. CHIEDE quindi alla Commissione di fare in modo che il mandato dell'ENISA teso a sostenere gli Stati membri e le istituzioni, gli organi e gli organismi dell'UE sia mirato e chiaramente definito, con obiettivi strategici concreti e compiti definiti in ordine di priorità, oltre a una ripartizione più precisa dei compiti e delle competenze rispetto ad altri attori. A tale riguardo, INVITA la Commissione a esaminare e rafforzare ulteriormente il ruolo dell'ENISA nel sostenere la cooperazione operativa a livello dell'UE e tra gli Stati membri al fine di rafforzarne la ciberresilienza, tenendo conto delle competenze degli Stati membri in questo settore. ESORTA inoltre la Commissione a rafforzare il ruolo consultivo dell'ENISA per quanto riguarda la fornitura di orientamenti e raccomandazioni di esperti e sulla base di dati concreti in relazione all'attuazione delle iniziative legislative e non legislative attuali e future dell'UE, garantendo nel contempo un quadro coerente dell'UE in materia di cibersicurezza.

5. Nello stesso spirito, INCORAGGIA la Commissione a valutare la possibilità di razionalizzare il ruolo dell'ENISA per quanto riguarda i compiti che non sono al centro della sua missione. SOTTOLINEA che le **responsabilità** dell'ENISA **sono state notevolmente ampliate** da recenti iniziative legislative, quali, tra l'altro, la direttiva NIS 2, il regolamento sulla ciberresilienza e il regolamento sulla cibersolidarietà. Pur RILEVANDO che l'ENISA ha ricevuto risorse aggiuntive a seguito di alcune delle suddette iniziative, SOTTOLINEA che l'ampliamento delle sue responsabilità e la crescente complessità delle minacce e delle sfide informatiche hanno portato a un notevole aumento dei suoi compiti, che dovrebbe tradursi in **risorse adeguate** — umane, finanziarie e tecniche —, al fine di consentire pienamente all'Agenzia di svolgere tutti i compiti di sua competenza, senza pregiudicare i negoziati sul quadro finanziario pluriennale. A tal fine, INVITA la Commissione, in sede di preparazione del progetto di bilancio generale dell'Unione, a definire un ordine di priorità delle azioni privilegiando i compiti che riguardano il sostegno agli Stati membri volto al rafforzamento della loro ciberresilienza, della loro cooperazione operativa e dello sviluppo e dell'attuazione del diritto dell'Unione.

SOSTEGNO DELL'ENISA ALLO SVILUPPO E ALL'ATTUAZIONE DELLE POLITICHE

6. RICORDA che, nell'ambito dell'attuale quadro giuridico in materia di cibersicurezza, all'ENISA sono affidate varie responsabilità fondamentali di sostegno e consulenza in tutta l'UE. A tale riguardo ACCOGLIE CON FAVORE il ruolo dell'ENISA volto a prestare **assistenza agli Stati membri** per l'attuazione efficace di iniziative legislative e non legislative. INVITA l'ENISA, in stretta collaborazione con il gruppo di cooperazione NIS e la Commissione, a continuare a fornire informazioni e analisi di portata generale sull'attuale contesto giuridico in materia di cibersicurezza. INCORAGGIA l'ENISA a condividere e promuovere attivamente orientamenti tecnici e migliori pratiche in modo regolare e strutturato, assistendo gli Stati membri nell'attuazione delle politiche e delle normative in materia di cibersicurezza.

7. RICONOSCE il ruolo fondamentale dell'ENISA nello sviluppo di **sistemi europei di certificazione della cibersicurezza** che promuovano la fiducia nei prodotti, nei servizi e nei processi TIC nonché nei servizi di sicurezza gestiti, alla luce dell'imminente modifica mirata del regolamento sulla cibersicurezza. SOTTOLINEA le preoccupazioni degli Stati membri e dell'industria per il lungo processo di selezione, elaborazione e adozione di sistemi di certificazione della cibersicurezza; ESORTA pertanto la Commissione a sfruttare l'opportunità offerta dalla valutazione del regolamento sulla cibersicurezza per trovare il modo di adottare un approccio basato sul rischio, più snello, più trasparente e più rapido per lo sviluppo di sistemi di certificazione della cibersicurezza dell'UE, SOTTOLINEANDO nel contempo l'importante ruolo degli Stati membri in questo esercizio. Inoltre, SOTTOLINEA l'importanza di attribuire esplicitamente la responsabilità del mantenimento di ciascun sistema di certificazione. RICORDA altresì che l'ENISA dovrebbe consultare tempestivamente tutti i portatori di interessi pertinenti attraverso un processo formale, aperto, trasparente e inclusivo nella fase di preparazione di proposte di sistemi e che la Commissione dovrebbe procedere a consultazioni aperte, trasparenti e inclusive al momento di valutare l'efficienza e l'uso dei sistemi adottati. INCORAGGIA l'ENISA a rafforzare ulteriormente la collaborazione con la comunità della protezione dei dati, in particolare il comitato europeo per la protezione dei dati, se del caso, e le autorità nazionali competenti, riservando un'attenzione particolare alla promozione di sinergie nel contesto dello sviluppo di futuri sistemi europei di certificazione della cibersicurezza.

8. Al fine di evitare inutili oneri amministrativi che potrebbero derivare da un quadro complesso in materia di comunicazione delle informazioni, INVITA l'ENISA, in cooperazione con la Commissione, a portare avanti gli scambi con gli Stati membri in merito agli aspetti pratici, alla semplificazione e alla razionalizzazione della procedura di comunicazione delle informazioni. RICORDA inoltre l'invito rivolto alla Commissione affinché prepari, con il sostegno dell'ENISA e di altri soggetti pertinenti dell'UE, una mappatura dei pertinenti obblighi di informazione stabiliti nei rispettivi atti legislativi dell'UE in materia informatica e digitale. RAMMENTA che lo scambio di informazioni tra l'ENISA e gli Stati membri si basa su un rapporto di fiducia, in cui la sicurezza e la riservatezza sono garantite conformemente al regolamento sulla cibersicurezza nonché alle norme e ai protocolli pertinenti, e dovrebbe essere limitato a quanto è pertinente e proporzionato ai fini di tale scambio. SOTTOLINEA la necessità che i dati e le informazioni siano trattati con la dovuta attenzione.

9. EVIDENZIA che l'ENISA è responsabile dell'istituzione e del mantenimento della **piattaforma unica di segnalazione ai sensi del regolamento sulla ciberresilienza**, che avrà un valore aggiunto operativo concreto, in particolare per le vulnerabilità attivamente sfruttate e gli incidenti gravi che incidono sulla sicurezza dei prodotti con elementi digitali. Dato l'ampio ambito di applicazione di tale normativa orizzontale, la piattaforma unica di segnalazione dovrebbe essere uno strumento efficace e sicuro per facilitare la condivisione delle informazioni tra i CSIRT nazionali e l'ENISA. Di conseguenza, ESORTA l'ENISA, oltre che a stanziare risorse umane sufficienti, ad accelerare l'istituzione della piattaforma quale priorità fondamentale al fine di garantirne l'operatività entro il termine fissato nel regolamento sulla ciberresilienza.

10. RICONOSCE il ruolo dell'ENISA nell'istituzione di una **banca dati europea delle vulnerabilità**, che mira a garantire una maggiore trasparenza per quanto riguarda la divulgazione delle vulnerabilità, garantendo nel contempo il trattamento adeguato dei dati sensibili. Considerando la fine del periodo di recepimento della direttiva NIS 2, ESORTA l'ENISA a intensificare tutti i lavori necessari per garantire il buon funzionamento di tale banca dati. In parallelo, INVITA il gruppo di cooperazione NIS, con l'assistenza dell'ENISA, a diffondere ulteriormente gli orientamenti, le politiche e le procedure in materia di divulgazione delle vulnerabilità.

11. RICONOSCE i vantaggi dell'**azione di sostegno alla cibersicurezza** condotta dall'ENISA, che funge da piattaforma comune per la fornitura di servizi di cibersicurezza agli Stati membri per integrarne gli sforzi, nonché dell'esperienza acquisita dall'ENISA con la sua attuazione. A tale riguardo, SOTTOLINEA che l'ENISA dovrebbe svolgere un ruolo centrale nell'amministrazione e nel funzionamento della riserva dell'UE per la cibersicurezza. INVITA l'ENISA ad avviare la mappatura dei servizi necessari e della loro disponibilità al momento stesso dell'entrata in vigore del regolamento sulla cibersolidarietà, al fine di rendere la riserva dell'UE per la cibersicurezza il più possibile utile e adattata alle esigenze degli utenti in tutti gli Stati membri. INVITA l'ENISA, una volta che le saranno stati assegnati i suoi compiti, a coinvolgere gli Stati membri, in particolare raccogliendo contributi sui criteri richiesti e informando in merito alle prossime gare d'appalto, nelle prime fasi del processo di istituzione della riserva dell'UE per la cibersicurezza. INVITA l'ENISA, una volta che le saranno stati assegnati i suoi compiti, a garantire che il processo di selezione dei fornitori di fiducia di servizi di sicurezza gestiti sia trasparente, aperto ed equo e consenta la partecipazione di fornitori di tutti gli Stati membri, indipendentemente dalle dimensioni. RICORDA inoltre che l'ENISA è tenuta a pubblicare senza indebito ritardo gli orientamenti in materia di interoperabilità per i poli informatici transfrontalieri.

12. SOTTOLINEA che il **monitoraggio delle tendenze relative alle tecnologie emergenti** in un settore in rapida evoluzione come il ciberspazio è di fondamentale importanza per mantenere e rafforzare ulteriormente la nostra posizione in materia di deterrenza informatica. RICONOSCE il lavoro svolto dall'ENISA nel richiamare l'attenzione del pubblico sui rischi e sulle possibilità di tecnologie quali l'intelligenza artificiale e la computazione quantistica, facilitando in tal modo una migliore comprensione delle sfide attuali. INCORAGGIA l'ENISA a contribuire ulteriormente a tali compiti, a sostenere attivamente l'attuazione delle sue raccomandazioni, nonché a fornire consulenza all'ECCC e a collaborare con lo stesso, se del caso.

SOSTEGNO DELL'ENISA AGLI STATI MEMBRI PER RAFFORZARE LA CIBERRESILIENZA E LA COOPERAZIONE OPERATIVA

13. SOTTOLINEA che l'ENISA svolge un ruolo importante **in qualità di segretariato delle due reti di cooperazione informatica guidate dagli Stati membri a livello dell'UE, ossia la rete CSIRT e EU-CyCLONe**. EVIDENZIA la preziosa partecipazione dell'ENISA al gruppo di cooperazione NIS, in particolare attraverso il suo coinvolgimento attivo e i suoi contributi tecnici nei vari filoni di lavoro. INCORAGGIA l'ENISA a continuare a sostenere il funzionamento e la cooperazione di tali reti in futuro, in quanto forniscono agli Stati membri canali fondamentali di collaborazione a diversi livelli.

14. RIBADISCE la necessità di migliorare la **conoscenza situazionale comune** a livello dell'UE, che contribuisce a definire la posizione dell'UE in materia di deterrenza informatica, in relazione al rilevamento e alla prevenzione degli incidenti di cibersicurezza nonché alla risposta agli stessi. A tale riguardo, SOTTOLINEA l'importanza delle attività di previsione dell'ENISA, delle relazioni periodiche e delle valutazioni delle minacce, tutti elementi che contribuiscono a migliorare la conoscenza situazionale. INCORAGGIA l'ENISA a collaborare strettamente con gli Stati membri per contribuire allo sviluppo di una conoscenza situazionale a livello dell'UE. In tale contesto RICONOSCE l'importante ruolo dell'ENISA, insieme al CERT-UE ed Europol, nel sostegno al Consiglio con briefing situazionali nel contesto del pacchetto di strumenti della diplomazia informatica che integrano la conoscenza situazionale fornita dalla capacità unica di analisi dell'intelligence (SIAC) e SOTTOLINEA la necessità di elaborare un quadro globale delle minacce provenienti da varie fonti, compreso il settore privato. INCORAGGIA, a tale proposito, l'ulteriore sviluppo della cooperazione dell'ENISA con il SEAE, in particolare con l'INTCEN, nel pieno rispetto dei rispettivi mandati.

15. SOTTOLINEA che il centro di situazione e analisi informatiche della Commissione svolge una funzione interna in seno alla Commissione ed è sostenuto dalla sua collaborazione con l'ENISA e il CERT-UE. Al fine di creare il massimo potenziale di sinergie e ridurre la complessità all'interno dell'ecosistema della cibersicurezza dell'UE, INVITA la Commissione a tenere conto dei risultati della valutazione del regolamento sulla cibersicurezza e delle discussioni sulla valutazione del programma per la cibersicurezza al fine di razionalizzare i compiti del centro di situazione e analisi informatiche della Commissione e i compiti correlati dell'ENISA. INCORAGGIA la Commissione a evitare inutili duplicazioni dei compiti, salvaguardando nel contempo il ruolo centrale dell'ENISA nel contribuire allo sviluppo di una conoscenza situazionale comune a livello dell'Unione a sostegno degli Stati membri, nel debito rispetto delle loro competenze nazionali.

16. EVIDENZIA che lo sviluppo di una conoscenza situazionale comune è un prerequisito per una gestione tempestiva ed efficace delle crisi dell'Unione nel suo complesso. RIMARCA che, a livello dell'UE, diversi attori chiave sono coinvolti nella **risposta agli incidenti di cibersicurezza su vasta scala** e che, in caso di tali incidenti, l'efficace cooperazione tra gli Stati membri è sostenuta principalmente dalla rete CSIRT e da EU-CyCLONe. L'ENISA svolge un ruolo importante nella gestione delle crisi informatiche in qualità di segretariato della rete CSIRT e di EU-CyCLONe. INVITA la Commissione a utilizzare la valutazione del programma per la cibersicurezza per rispecchiare adeguatamente i compiti e le responsabilità supplementari in termini di contributo allo sviluppo di una risposta cooperativa agli incidenti o alle crisi su vasta scala in materia di cibersicurezza, nonché il ruolo attribuito all'ENISA in qualità di segretariato della rete CSIRT e di EU-CyCLONe e dalla recente legislazione in materia di cibersicurezza.

17. SOTTOLINEA l'importanza di organizzare periodicamente **esercitazioni di cibersicurezza** che aumentino notevolmente la preparazione dell'UE nella risposta agli incidenti e alle crisi. RICONOSCE che l'ENISA ha acquisito una preziosa e vasta esperienza in questo settore a sostegno degli Stati membri. PRENDE ATTO dell'importante ruolo svolto dall'ENISA nelle fasi di pianificazione, preparazione, esecuzione e valutazione delle esercitazioni di cibersicurezza e SOTTOLINEA che tale Agenzia dovrebbe continuare a rimanere uno degli attori centrali a livello dell'UE, tenendo presente che tali esercitazioni dovrebbero essere effettuate sulla base di quadri strutturati e terminologie comuni. INVITA l'ENISA, la rete CSIRT e EU-CyCLONe a utilizzare nel modo più efficiente possibile le esercitazioni periodiche esistenti per testare e migliorare il quadro di risposta alle crisi dell'UE e a garantire la massima diffusione degli insegnamenti tratti.

COOPERAZIONE DELL'ENISA CON ALTRI ATTORI DELL'ECOSISTEMA DELLA CIBERSICUREZZA

18. RIBADISCE che, data la natura orizzontale della cibersicurezza, è essenziale una **collaborazione tra tutti gli attori a livello degli Stati membri e dell'Unione** e SOTTOLINEA pertanto che l'aumento della ciberresilienza globale a livello europeo richiede anche un lavoro congiunto tra l'ENISA e altri soggetti pertinenti nel settore della cibersicurezza.

19. SOTTOLINEA che la capacità delle istituzioni, degli organi e degli organismi dell'UE di continuare a garantire la loro cibersicurezza è importante per la ciberresilienza globale a livello dell'UE, alla quale il CERT-UE contribuisce in modo determinante. A tale riguardo, ACCOGLIE CON FAVORE la cooperazione strutturata instaurata tra il CERT-UE e l'ENISA e li INCORAGGIA a proseguire la loro stretta cooperazione in futuro.

20. Grazie all'autonomia finanziaria raggiunta, l'ECCC contribuirà in modo significativo allo sviluppo di un solido ecosistema europeo della cibersicurezza in ambito industriale, tecnologico e della ricerca, comprendente competenze per lo sviluppo della forza lavoro in linea con il suo mandato. INCORAGGIA l'ENISA e l'ECCC a proseguire la loro stretta cooperazione, in particolare in relazione alle esigenze e alle priorità in materia di ricerca e innovazione, nonché alle competenze in materia di cibersicurezza, al fine di aumentare la competitività dell'industria della cibersicurezza nell'Unione. INVITA la Commissione a esaminare in che modo le sinergie nel funzionamento dell'ENISA e dell'ECCC possano essere ulteriormente ottimizzate e come razionalizzare meglio le attività secondo i rispettivi mandati.

21. SOTTOLINEA che la fornitura di aggiornamenti periodici sul panorama delle minacce contribuisce a individuare meglio le misure e gli strumenti necessari per combattere efficacemente la cibercriminalità. SOTTOLINEA il valore aggiunto delle relazioni di valutazione congiunta per il ciberspazio (J-CAR) dell'UE, che sono il risultato della collaborazione congiunta tra l'ENISA, l'EC3 di Europol e il CERT-UE e hanno già fornito un prezioso contributo nell'affrontare le diverse sfide, compresa la lotta alla cibercriminalità. INVITA l'ENISA ed Europol a continuare a collaborare in modo strutturato in futuro.

22. SOTTOLINEA che la ciberdifesa costituisce un elemento importante e in continua evoluzione della lotta alle minacce derivanti dal ciberspazio. EVIDENZIA la necessità che l'ENISA collabori con il SEAE e la Commissione nei casi in cui l'ENISA svolge un ruolo nel sostenere l'attuazione della politica dell'UE in materia di ciberdifesa, in stretta cooperazione con l'AED, l'ECCC e la comunità di ciberdifesa. PONE L'ACCENTO sul ruolo dell'ENISA in quanto agenzia civile. SOTTOLINEA l'importanza di approfondire e razionalizzare la cooperazione civile-militare nel settore della cibersicurezza all'interno dell'UE, comprese chiare divisioni dei ruoli e delle responsabilità tra le due comunità e tra l'UE e la NATO, nel pieno rispetto dei principi di inclusività, reciprocità, apertura reciproca e trasparenza, nonché dell'autonomia decisionale di entrambe le organizzazioni. INCORAGGIA l'ENISA a continuare a perseguire accordi di lavoro con l'Agenzia della NATO per le comunicazioni e l'informazione.

23. INCORAGGIA l'UE a continuare a promuovere i nostri valori comuni e i nostri sforzi congiunti nei consessi globali al fine di salvaguardare un ciberspazio libero, globale, aperto e sicuro. SOTTOLINEA che la natura transfrontaliera delle minacce e degli incidenti informatici richiede una collaborazione forte ed efficace, non solo a livello dell'UE, ma anche con **organizzazioni e partner internazionali**. OSSERVA che il coinvolgimento internazionale dell'ENISA dovrebbe concentrarsi sui partner strategici e sui paesi candidati all'adesione all'UE, in linea con la politica estera e di sicurezza comune dell'UE. EVIDENZIA che, nel suo coinvolgimento internazionale, l'ENISA dovrebbe agire conformemente al suo mandato e alle rispettive disposizioni del regolamento sulla cibersicurezza. RICONOSCE la necessità di chiarire, conformemente alle procedure pertinenti, il coinvolgimento internazionale dell'ENISA, garantendo in particolare che il suo consiglio di amministrazione sia debitamente e tempestivamente informato delle attività correlate. INCORAGGIA il coinvolgimento dell'ENISA nei pertinenti quadri internazionali di cooperazione in materia di cibersicurezza, anche nell'ambito di organizzazioni quali la NATO e l'OSCE.

24. RIBADISCE che l'UE e i suoi Stati membri hanno spesso evidenziato lacune nelle **competenze in materia di cibersicurezza**. RICORDA che la Commissione e l'ENISA hanno introdotto un quadro ampio e generale per fornire orientamenti a tutti i portatori di interessi, comprendente in particolare il quadro europeo in materia di competenze nel settore della cibersicurezza, la comunicazione sull'Accademia per le competenze in materia di cibersicurezza e la conferenza europea sulle competenze in materia di cibersicurezza, organizzata annualmente, e INCORAGGIA la Commissione e l'ENISA a prendere le mosse da tali iniziative, con particolare riguardo alla discussione in corso sul consorzio per l'infrastruttura digitale europea (EDIC). A tal fine, INVITA la Commissione a coordinarsi con gli Stati membri interessati a istituire un EDIC. RICONOSCE che sia l'ENISA che l'ECCC hanno il compito di promuovere le competenze in tutta l'Unione. INVITA l'ENISA a dare priorità a sostenere gli sforzi degli Stati membri in materia di competenze e istruzione, a rafforzare la sensibilizzazione del grande pubblico e, se del caso, a collaborare con l'ECCC.

25. RICONOSCE che negli ultimi anni l'ENISA ha sviluppato una **cooperazione con il settore privato**. RICORDA che, poiché il settore privato monitora costantemente il panorama delle minacce informatiche, le informazioni raccolte dall'industria potrebbero contribuire a migliorare la conoscenza situazionale comune. INCORAGGIA pertanto l'ENISA, in stretta cooperazione con gli Stati membri e i soggetti di tutta l'UE, a rafforzare la cooperazione con il settore privato.

26. INVITA la Commissione e l'ENISA a valutare modalità per rafforzare la collaborazione tra l'ENISA e le organizzazioni europee di **normazione**. SOTTOLINEA la necessità che l'ENISA aumenti le proprie competenze in materia di normazione europea relativa alla cibersicurezza, tra l'altro dando seguito e partecipando alle attività di normazione.

27. ESORTA la Commissione e l'ENISA a esaminare come ottimizzare ulteriormente il funzionamento del quadro dell'UE in materia di cibersicurezza, tenendo conto delle raccomandazioni e delle proposte formulate nelle presenti conclusioni. La cooperazione continua, la definizione delle priorità in termini di compiti e risorse e la semplificazione del complesso panorama della cibersicurezza saranno elementi chiave per far fronte alle sfide attuali e future.