Consiglio
dell'Unione europea

Bruxelles, 17 ottobre 2022
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	17 ottobre 2022
Destinatario:	Delegazioni
n. doc. prec.:	12930/22
Oggetto:	Conclusioni del Consiglio sulla sicurezza della catena di approvvigionamento delle TIC - Conclusioni del Consiglio approvate dal Consiglio nella sessione del 17 ottobre 2022

Si allegano per le delegazioni le conclusioni del Consiglio sulla sicurezza della catena di approvvigionamento delle TIC, approvate dal Consiglio nella sessione tenutasi il 17 ottobre 2022.

ALLEGATO

Conclusioni del Consiglio sulla sicurezza della catena di approvvigionamento delle TIC

IL CONSIGLIO DELL'UNIONE EUROPEA,

RAMMENTANDO le sue conclusioni:

– sulla comunicazione congiunta al Parlamento europeo e al Consiglio: "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE" del 20 novembre 2017;

– sullo sviluppo di capacità e competenze in materia di cibersicurezza nell'UE;

– sull'importanza del 5G per l'economia europea e sulla necessità di attenuare i relativi rischi per la sicurezza;

– "Plasmare il futuro digitale dell'Europa";

– "Una ripresa che fa progredire la transizione verso un'industria europea più dinamica, resiliente e competitiva";

– sulla cibersicurezza dei dispositivi connessi;

– sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale;

– sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica;

– sulla relazione speciale n. 03/2022 della Corte dei conti europea dal titolo "L'introduzione del 5G nell'UE: vi sono ritardi nel dispiegamento delle reti e le questioni di sicurezza rimangono irrisolte";

RICORDANDO le conclusioni del Consiglio europeo sui seguenti temi:

– COVID-19, mercato unico, politica industriale, digitale e relazioni esterne, del 1º e 2 ottobre 2020;

– aggressione militare russa nei confronti dell'Ucraina, sicurezza e difesa, energia, questioni economiche, COVID-19 e relazioni esterne, del 24 e 25 marzo 2022;

– Ucraina, sicurezza alimentare, sicurezza e difesa ed energia, del 30 e 31 maggio 2022;

1. SOTTOLINEA, data la crescente importanza della geopolitica per la cibersicurezza, che l'Unione europea e i suoi Stati membri devono affrontare la cibersicurezza in modo globale e strategico. L'aggressione militare russa nei confronti dell'Ucraina ha provocato un cambiamento significativo del contesto strategico e di sicurezza dell'Unione europea e ha messo in luce la necessità di un'Unione europea più forte e capace nel settore della sicurezza e della difesa. Ha sottolineato che è della massima importanza tenere adeguatamente conto del contesto geopolitico non solo nel reagire alle attività informatiche malevole, ma anche nel costruire e mantenere la resilienza delle tecnologie dell'informazione e della comunicazione (TIC). Tale aspetto riveste particolare importanza per le catene di approvvigionamento di prodotti e servizi TIC (catene di approvvigionamento delle TIC), che potrebbero essere compromesse sia sulla base della rivalità geopolitica, come illustrato dall'attacco SolarWinds, sia a causa delle tensioni geopolitiche e dell'instabilità, come dimostrato dalla minaccia legata alla dipendenza dai fornitori russi di TIC al momento dell'aggressione militare russa nei confronti dell'Ucraina.

2. OSSERVA che la natura dei rischi associati alla catena di approvvigionamento delle TIC, che è composta di un insieme collegato di risorse e processi tra operatori economici (quali definiti nel regolamento (UE) 2019/1020), che inizia con l'approvvigionamento di materie prime e si estende alla fabbricazione, trasformazione, manipolazione e fornitura di prodotti e servizi TIC, compresa la prestazione di supporto durante il ciclo di vita dei prodotti e dei servizi TIC, comporta sfide uniche e conseguenze potenzialmente di vasta portata. Oltre ai rischi connessi all'indisponibilità di prodotti TIC, ad esempio a causa delle carenze di materie prime critiche e di semiconduttori necessari per la loro produzione, le catene di approvvigionamento di prodotti e servizi TIC sono esposte ad altre minacce. In particolare, possono essere prese di mira o utilizzate impropriamente da soggetti malintenzionati che ricorrono a metodi sofisticati e spesso occulti che hanno un impatto sulla riservatezza, l'integrità e la disponibilità di dati sensibili trasmessi e conservati.

3. Riconoscendo la necessità di un approccio multirischio per mettere al sicuro le risorse TIC, RICONOSCE l'importanza della proposta di direttiva sulla resilienza dei soggetti critici per migliorare la sicurezza fisica di detti soggetti e SOTTOLINEA che, oltre a rafforzare la resilienza contro gli attacchi alle catene di approvvigionamento perpetrati con mezzi informatici, è altrettanto importante rafforzare la resilienza e la sicurezza complessive delle catene di approvvigionamento delle TIC nei confronti dell'intera gamma di fattori di minaccia, quali eventi naturali, disfunzioni del sistema, minacce interne o errori umani. In tal senso, RICONOSCE che la sicurezza della catena di approvvigionamento delle TIC comprende la garanzia della protezione dei prodotti e dei servizi TIC realizzati, forniti, acquistati e utilizzati nelle catene di approvvigionamento delle TIC, anche attraverso la protezione dei singoli componenti e dei dati trasmessi.

4. Sulla base degli insegnamenti tratti dalle conseguenze delle dipendenze strategiche dell'Unione europea dai combustibili fossili russi e dagli impatti delle interruzioni delle catene di approvvigionamento durante la pandemia di COVID-19, in particolare in relazione ai prodotti farmaceutici e ai semiconduttori, da cui sono emerse le dipendenze strategiche dell'UE, INCORAGGIA gli Stati membri ad adoperarsi per evitare situazioni analoghe di dipendenze esterne strategiche indesiderate in relazione ai prodotti e ai servizi TIC. A causa della crescente digitalizzazione della società e dell'utilizzo sempre maggiore delle TIC nelle infrastrutture critiche, le dipendenze esterne strategiche connesse ai prodotti e ai servizi TIC e alle loro catene di approvvigionamento dovrebbero essere costantemente valutate e, se del caso, affrontate.

5. RICORDA che conseguire l'autonomia strategica preservando nel contempo un'economia aperta è un obiettivo fondamentale dell'Unione che comprende l'individuazione e la riduzione delle dipendenze strategiche e l'aumento della resilienza negli ecosistemi industriali più sensibili e in settori specifici, compreso quello digitale. Ciò comprende lo sviluppo e la diffusione di capacità e infrastrutture digitali strategiche, il rafforzamento della capacità di compiere scelte tecnologiche autonome e — in quanto uno dei pilastri principali — la garanzia di infrastrutture, prodotti e servizi resilienti e sicuri per accrescere la fiducia nel mercato unico digitale e all'interno della società europea, mantenendo nel contempo l'apertura, la cooperazione globale con i partner che condividono gli stessi principi e la competitività, e sfruttando i potenziali benefici che ne derivano. I valori fondamentali dell'Unione europea preservano in particolare la vita privata, la sicurezza, l'uguaglianza, la dignità umana, lo Stato di diritto e l'internet aperta come prerequisiti per realizzare una società, un'economia e un'industria antropocentriche e orientate al settore digitale.

6. OSSERVA che, a causa degli sviluppi nel panorama delle minacce informatiche dimostrati dalla tendenza ad attacchi di forte impatto e altamente sofisticati alle catene di approvvigionamento negli ultimi anni (come gli attacchi SolarWinds, Mimecast o Kaseya), concomitanti all'esternalizzazione di servizi TIC essenziali e intensificati dalla dipendenza generale da prodotti e servizi TIC realizzati, forniti o prestati da terzi, è altamente probabile che in futuro si verifichino più attacchi alla catena di approvvigionamento, con danni sostanziali per l'economia e la società. Alla luce di quanto precede, SOTTOLINEA l'importanza di rafforzare la sicurezza e la resilienza delle catene di approvvigionamento delle TIC per il funzionamento del mercato unico, unitamente alla necessità di garantire la disponibilità, la sicurezza e la diversità dei prodotti e dei servizi TIC nel mercato unico. RICONOSCE pertanto la necessità di massimizzare e razionalizzare l'uso degli strumenti e degli approcci esistenti nell'UE per conseguire tali obiettivi, nonché l'esigenza di adattarsi costantemente all'evoluzione del panorama delle minacce informatiche introducendo misure e meccanismi supplementari adeguati, anche in relazione ai possibili rischi per la sicurezza posti da tecnologie emergenti e di rottura. INCORAGGIA gli Stati membri a perseguire, a tale riguardo, un approccio basato sul rischio per affrontare i nuovi sviluppi tecnologici.

7. RICONOSCE che comprendere il panorama delle minacce informatiche — che è in costante evoluzione — e la complessità degli attacchi alla catena di approvvigionamento è essenziale per attenuare efficacemente i rischi associati alle catene di approvvigionamento delle TIC. A tale riguardo, SOTTOLINEA la necessità di adeguarsi alle nuove minacce monitorando, analizzando e valutando in modo attivo e continuo il panorama delle minacce alla catena di approvvigionamento, di sensibilizzare e sviluppare conoscenze sulle minacce e le vulnerabilità, nonché di allertare in modo proattivo e mirato i soggetti pertinenti. ACCOGLIE CON FAVORE il lavoro dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) relativo alla sicurezza della catena di approvvigionamento delle TIC, in particolare la sua relazione sul panorama delle minacce sotto forma di attacchi alla catena di approvvigionamento.

STRUMENTI E APPROCCI INTERSETTORIALI

8. RIBADISCE l'importanza che gli Stati membri tengano conto della necessità di diversificare i fornitori di TIC critiche al fine di evitare o limitare la creazione di forti dipendenze da singoli fornitori, in particolare da fornitori ad alto rischio, in quanto ciò aumenta l'esposizione alle conseguenze di potenziali interruzioni. RICONOSCE che l'assenza di pratiche di *lock-in* e la diversificazione dei fornitori di TIC costituiscono una delle componenti importanti per garantire la stabilità e la sicurezza del mercato interno. SOTTOLINEA la necessità di promuovere e attuare strategie adeguate che facilitino la diversificazione dei venditori e la competitività in modo tecnologicamente neutro. INCORAGGIA inoltre a integrare nella legislazione dell'UE gli aspetti relativi alla prevenzione delle pratiche di *lock-in*. A tale proposito, PRENDE ATTO della proposta di regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), volto ad accrescere l'interoperabilità dei servizi di trattamento dei dati e a rimuovere gli ostacoli al passaggio tra fornitori di servizi di trattamento dei dati.

9. RICONOSCE il nesso tra la sicurezza della catena di approvvigionamento delle TIC e gli appalti pubblici. SOTTOLINEA la necessità che le procedure di appalto pubblico tengano adeguatamente conto dell'importanza della sicurezza della catena di approvvigionamento delle TIC imponendo, se del caso, criteri di selezione oggettivi e basati sul rischio relativi alla capacità degli offerenti di garantire un elevato livello di sicurezza dei servizi forniti. CHIEDE di trovare il giusto equilibrio tra, da un lato, l'interesse pubblico all'utilizzo più efficiente ed equo dei fondi pubblici e, dall'altro, l'interesse pubblico a garantire la sicurezza dei sistemi di informazione e il buon funzionamento del mercato unico. Per agevolare l'attuazione delle pertinenti norme in materia di appalti pubblici alla luce dell'aumento della cibersicurezza, INVITA la Commissione a elaborare orientamenti metodologici entro il terzo trimestre del 2023 al fine di incoraggiare le amministrazioni aggiudicatrici a prestare un'adeguata attenzione alle pratiche degli offerenti e dei relativi subappaltatori in materia di cibersicurezza, nonché a valutare e, se necessario, presentare proposte volte a rivedere o integrare la pertinente normativa in materia di appalti pubblici.

10. RICONOSCE che gli investimenti esteri diretti connessi a prodotti e servizi TIC, pur fornendo benefici economici e sociali agli Stati membri, alle imprese e ai cittadini, potrebbero comportare rischi per la sicurezza e l'ordine pubblico e RILEVA che il meccanismo di controllo degli investimenti esteri diretti dell'UE, unitamente ai rispettivi regimi nazionali di controllo — che forniscono mezzi per far fronte a tali rischi —, potrebbe altresì costituire uno strumento utile per salvaguardare la sicurezza e la resilienza della catena di approvvigionamento delle TIC contribuendo a rimuovere gli investimenti ad alto rischio che possono incidere su sicurezza e resilienza. RICONOSCE che le informazioni scambiate e condivise mediante questo meccanismo possono aiutare gli Stati membri a valutare meglio le possibili minacce alla sicurezza delle catene di approvvigionamento delle TIC e ad adottare le opportune misure necessarie. INVITA i soggetti nazionali competenti a tenere altresì conto di questa dimensione del meccanismo di controllo, se del caso.

11. Per quanto concerne la difesa, RIBADISCE l'invito rivolto alla Commissione a valutare nel 2023, insieme agli Stati membri, i rischi per le catene di approvvigionamento delle infrastrutture critiche in vari settori, compreso quello digitale, inerenti agli interessi dell'UE in materia di sicurezza e difesa, nonché a vagliare opzioni per accrescere la cibersicurezza nell'intera catena di approvvigionamento della base industriale e tecnologica di difesa dell'UE. Inoltre, INVITA gli Stati membri e la Commissione a riflettere sulla sicurezza della catena di approvvigionamento delle TIC nell'attuazione degli impegni e delle azioni della bussola strategica.

12. Riconoscendo l'importanza delle materie prime critiche e di tutti i tipi di semiconduttori quali elementi costitutivi di base dei prodotti TIC, INCORAGGIA l'avvio di negoziati costruttivi sulla proposta di regolamento che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori (normativa sui chip) e sulla proposta di regolamento del Consiglio recante modifica del regolamento (UE) 2021/2085 che istituisce le imprese comuni nell'ambito di Orizzonte Europa per quanto riguarda l'impresa comune "Chip".

STRUMENTI SPECIFICI DEL CIBERSPAZIO

13. Per quanto riguarda nello specifico l'infrastruttura di telecomunicazione, RICONOSCE i risultati conseguiti a livello dell'Unione per migliorare la sicurezza della catena di approvvigionamento delle reti 5G, in particolare attraverso il pacchetto di strumenti dell'UE per la sicurezza del 5G (pacchetto di strumenti dell'UE per il 5G). INVITA gli Stati membri a proseguire lo scambio di informazioni sulle migliori prassi e metodologie relativamente all'attuazione delle misure indicate nel pacchetto di strumenti dell'UE per il 5G e in particolar modo ad applicare le pertinenti restrizioni ai fornitori ad alto rischio per gli asset chiave, definiti critici e sensibili nella valutazione dei rischi coordinata a livello dell'UE. SOTTOLINEA che il pacchetto di strumenti dell'UE per il 5G rappresenta uno strumento agile basato sul rischio per affrontare le sfide individuate in materia di sicurezza, che consente di gestire gli aspetti relativi alla cibersicurezza del 5G in modo tempestivo ed efficiente, nel rispetto delle competenze degli Stati membri, e RICONOSCE che si tratta di uno strumento prezioso per accrescere ulteriormente, in totale trasparenza, la sicurezza della catena di approvvigionamento delle reti di telecomunicazione in un modo coordinato che potrebbe servire da ispirazione per gli strumenti di valutazione e attenuazione dei rischi relativi ad altri settori vitali. RICORDA l'invito indirizzato alle autorità competenti a formulare, sulla base di valutazioni dei rischi, raccomandazioni rivolte agli Stati membri e alla Commissione con l'obiettivo di rafforzare la resilienza delle reti e infrastrutture di comunicazione nell'Unione europea, ivi compreso il proseguimento dell'attuazione del pacchetto di strumenti dell'UE per il 5G.

14. RILEVA l'importanza di approcci interoperabili che possano affrontare le pratiche di *lock-in* e diluire il rischio di concentrazione, migliorando nel contempo la sicurezza della catena di approvvigionamento nell'intera gamma di infrastrutture e servizi TIC. Per quanto concerne nello specifico le reti 5G, RICONOSCE i potenziali benefici del concetto di Open RAN a tale riguardo e al tempo stesso RAMMENTA la relazione sulla cibersicurezza di Open RAN pubblicata dal gruppo di cooperazione NIS in cui si osserva che tale concetto è ancora in fase di sviluppo e che la sua sicurezza, trasparenza e standardizzazione sono in una fase iniziale di maturità; SOTTOLINEA poi l'importanza di valutare i rischi prima di qualsiasi transizione verso nuovi standard o architetture.

15. SOTTOLINEA l'importanza degli strumenti legislativi orizzontali — esistenti e futuri — in materia di cibersicurezza, in particolare il regolamento relativo all'ENISA (l'Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (regolamento sulla cibersicurezza), l'imminente direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS 2), la proposta di regolamento che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione, nonché la proposta di regolamento sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (normativa sulla ciberresilienza), per aumentare la sicurezza della catena di approvvigionamento delle TIC. PRENDE ATTO inoltre degli importanti sviluppi nelle normative settoriali in materia di cibersicurezza, in particolare il futuro regolamento sulla resilienza operativa digitale per il settore finanziario (DORA), che comprende un quadro di sorveglianza per i fornitori terzi di servizi TIC che sono critici per le entità finanziarie. Tali normative prevedono obblighi generali relativi alla sicurezza della catena di approvvigionamento nonché requisiti dettagliati e specifici attinenti al settore interessato. Al tempo stesso SOTTOLINEA che i fornitori spesso offrono i loro prodotti e servizi a settori differenti, piuttosto che ad una singola industria. È quindi molto importante garantire che i requisiti di sicurezza della catena di approvvigionamento siano, per quanto possibile, allineati in tutti i pertinenti settori, segnatamente quelli contemplati dalla futura direttiva NIS 2, al fine di evitare discrepanze tra gli obblighi imposti ai fornitori e alleggerire l'onere, gravante sugli operatori dei settori critici, di valutare il rispetto di tali obblighi da parte dei fornitori, tenendo conto nel contempo delle specificità settoriali.

16. ACCOGLIE CON FAVORE la proposta di normativa sulla ciberresilienza quale importante strumento legislativo per promuovere lo sviluppo sicuro di prodotti con elementi digitali e per fare in modo che si tenga conto della cibersicurezza nell'intero ciclo di vita dei prodotti con elementi digitali. OSSERVA che la proposta di normativa sulla ciberresilienza può contribuire in modo significativo ad accrescere la sicurezza della catena di approvvigionamento delle TIC. INCORAGGIA l'avvio di negoziati costruttivi e l'adozione tempestiva della normativa.

17. A tal proposito RICONOSCE i lavori in corso condotti dall'ENISA, insieme agli Stati membri e ad altri portatori di interessi, per fornire all'UE sistemi di certificazione per i prodotti, i servizi e i processi TIC, in linea con il regolamento sulla cibersicurezza, che dovrebbero contribuire a innalzare il livello complessivo della cibersicurezza all'interno del mercato unico digitale. INCORAGGIA tutti i portatori di interessi a partecipare ai lavori preparatori sui singoli sistemi europei di certificazione al fine di creare fiducia nei confronti di prodotti, processi e servizi TIC sicuri e di rafforzarne la resilienza e INVITA la Commissione a elaborare rapidamente, dopo il completamento dei lavori preparatori, atti di esecuzione in materia di sistemi europei di certificazione, nello specifico il sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC). RILEVA che i sistemi europei di certificazione dovrebbero includere, se necessario, requisiti in materia di sicurezza della catena di approvvigionamento, ivi compresi i rapporti con i fornitori.

18. EVIDENZIA la necessità di dare completa attuazione a tutte le disposizioni connesse alla sicurezza della catena di approvvigionamento delle TIC contenute nella prossima direttiva NIS 2. A tale proposito SOTTOLINEA l'importanza delle valutazioni dei rischi, coordinate a livello dell'UE, delle catene di approvvigionamento critiche (valutazioni coordinate dei rischi delle catene di approvvigionamento), di politiche nazionali in materia di sicurezza delle catene di approvvigionamento e di misure di sicurezza connesse alle catene di approvvigionamento. RILEVA che è opportuno prestare attenzione non solo ai fornitori primari, ma anche ai relativi subappaltatori per quanto riguarda i rischi per la sicurezza del fornitore primario o del cliente finale. Al fine di agevolare l'attuazione di misure di gestione dei rischi della catena di approvvigionamento, INCORAGGIA l'ENISA a fare, con l'aiuto del gruppo di cooperazione NIS, un bilancio delle migliori prassi disponibili per la gestione dei rischi della catena di approvvigionamento e a raccogliere tali buone prassi in linee guida metodologiche. INCORAGGIA altresì l'ENISA a monitorare gli investimenti nella sicurezza della catena di approvvigionamento delle TIC dei soggetti regolamentati dalla prossima direttiva NIS 2.

19. EVIDENZIA inoltre i benefici e i rischi derivanti dall'utilizzo, nel contesto della sicurezza della catena di approvvigionamento, di fornitori di servizi gestiti e di fornitori di servizi di sicurezza gestiti. Sebbene il ricorso a detti fornitori possa migliorare considerevolmente la sicurezza all'interno delle organizzazioni e garantire livelli più elevati di cibersicurezza, la gestione remota dei sistemi e dei servizi TIC combinata all'accesso privilegiato all'ambiente TIC dei clienti, di cui i fornitori di servizi gestiti e i fornitori di servizi di sicurezza gestiti potrebbero avere bisogno, può avere notevoli effetti a cascata su un elevato numero di clienti, nel caso in cui siano compromessi i fornitori di servizi gestiti o i fornitori di servizi di sicurezza gestiti. È pertanto della massima importanza che i fornitori di servizi gestiti e i fornitori di servizi di sicurezza gestiti mantengano un elevato livello sia della propria sicurezza interna che della sicurezza dei servizi da loro forniti e che adottino un approccio trasparente nei confronti dei propri clienti per quanto riguarda la sicurezza dei servizi che forniscono. ACCOGLIE CON FAVORE, a tale proposito, la loro futura inclusione nell'ambito di applicazione della prossima direttiva NIS 2.

20. Per quanto riguarda l'attuazione del meccanismo di valutazione coordinata dei rischi legati alla catena di approvvigionamento ai sensi della prossima direttiva NIS 2, RILEVA la pertinenza dei fattori di rischio non tecnici in questo contesto, quali l'indebita influenza di uno Stato terzo sui fornitori e sui fornitori di servizi, e, a tal proposito, RICONOSCE i fattori che possono essere utilizzati per valutare il profilo di rischio menzionato nella valutazione dei rischi coordinata a livello dell'UE della cibersicurezza delle reti 5G. INVITA la Commissione a individuare, entro il secondo trimestre del 2023 e previa consultazione del gruppo di cooperazione NIS e dell'ENISA, gli specifici servizi, sistemi o prodotti TIC che potrebbero essere in via prioritaria oggetto delle valutazioni coordinate dei rischi legati alla catena di approvvigionamento.

21. RILEVA che la dipendenza da fornitori ad alto rischio di prodotti e servizi TIC utilizzati per il funzionamento di reti e sistemi critici rappresenta una minaccia strategica che deve essere attenuata introducendo opportune politiche a livello sia nazionale che dell'UE e ricorrendo alla cooperazione tra Stati membri e con partner internazionali che condividono gli stessi principi. Al fine di agevolare l'attenuazione di tale rischio strategico e sostenere le valutazioni coordinate dei rischi legati alla catena di approvvigionamento, INVITA il gruppo di cooperazione NIS, in cooperazione con la Commissione e l'ENISA, a elaborare un pacchetto di misure tese a ridurre i rischi critici della catena di approvvigionamento delle TIC (pacchetto di strumenti per la catena di approvvigionamento delle TIC). Il pacchetto di strumenti per la catena di approvvigionamento delle TIC dovrebbe partire da scenari di minaccia strategici individuati per le catene di approvvigionamento delle TIC e prevedere, in risposta a detti scenari, misure che fanno leva sulle esperienze acquisite con il pacchetto di strumenti per il 5G e a livello nazionale. Dovrebbe integrare in modo trasparente le valutazioni coordinate dei rischi legati alla catena di approvvigionamento per specifici servizi, sistemi o prodotti TIC a norma della prossima direttiva NIS 2, offrendo misure generiche per la riduzione dei rischi che possono essere adeguate in modo scalabile per specifici servizi, sistemi o prodotti TIC, sulla base dei rischi individuati nelle singole valutazioni coordinate dei rischi legati alla catena di approvvigionamento.

22. SOTTOLINEA l'importante ruolo che svolgono la ricerca, l'innovazione, gli investimenti e le attività imprenditoriali nel settore digitale e della cibersicurezza, come anche il finanziamento di tali attività, nell'evitare eventuali dipendenze strategiche future indesiderate e nel rafforzare la resilienza complessiva delle catene di approvvigionamento delle TIC. In tale contesto, PONE L'ACCENTO sul ruolo e sulla pertinenza dei compiti sia strategici che attuativi del Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca (ECCC) e della rete dei centri nazionali di coordinamento nel contribuire a massimizzare gli effetti degli investimenti per rafforzare la leadership e l'autonomia strategica aperta dell'Unione nel settore della cibersicurezza, per sostenere le capacità e le competenze tecnologiche dell'Unione e per accrescere la competitività globale dell'Unione. A tale proposito INVITA a rendere rapidamente operativo l'ECCC. INVITA l'ECCC a tenere conto, nella sua agenda strategica, degli aspetti relativi alla sicurezza della catena di approvvigionamento delle TIC, ivi compresi, ad esempio, lo sviluppo di software sicuro, garantendo nel contempo coerenza e complementarità ed evitando qualsiasi duplicazione degli sforzi. SOSTIENE l'aumento della competitività europea nel settore della cibersicurezza attraverso programmi di finanziamento, quali il programma di ricerca e innovazione Orizzonte Europa e il programma Europa digitale per rafforzare, costruire e acquisire capacità essenziali per l'economia, la società e la democrazia dell'UE.

MECCANISMI DI SOSTEGNO

23. INCORAGGIA il potenziamento degli incentivi di sostegno finanziario connessi alle misure volte a rafforzare la sicurezza della catena di approvvigionamento delle TIC. INVITA in via prioritaria l'ECCC, la Commissione e i pertinenti portatori di interessi, anche in vista della prossima attuazione della direttiva NIS 2, a vagliare opzioni per includere gli aspetti relativi alla sicurezza della catena di approvvigionamento delle TIC nei prossimi inviti a presentare proposte nell'ambito dei programmi di lavoro in materia di cibersicurezza a titolo dei programmi Europa digitale e Orizzonte Europa, o qualsiasi altra opportunità di finanziamento pertinente. Tali opportunità di finanziamento dovrebbero, tra l'altro, essere volte a consentire alle organizzazioni di sostenere il mantenimento di un elevato livello di cibersicurezza in termini di approvvigionamento di prodotti e servizi TIC lungo tutta la catena di approvvigionamento, in particolare in relazione alla sostituzione di specifici servizi, sistemi o prodotti TIC critici, riconosciuti ad alto rischio in conformità delle future valutazioni coordinate dei rischi legati alla catena di approvvigionamento.

24. RICONOSCE che la globalizzazione e la specializzazione dei servizi TIC nonché la maggiore dipendenza da prodotti e servizi di terzi comportano la necessità di una stretta cooperazione all'interno dell'UE e a livello internazionale nella condivisione delle conoscenze e delle competenze tra i pertinenti portatori di interessi e li INCORAGGIA a trovare una posizione forte e coordinata che garantisca la sicurezza della catena di approvvigionamento delle TIC in modo globale. RICONOSCE inoltre la necessità di esplorare ulteriormente gli approcci e le tecniche all'avanguardia pertinenti, sia per un'igiene informatica di base adeguata che per soluzioni a lungo termine volte a conseguire catene di approvvigionamento delle TIC sicure e resilienti, nonché le modalità più adeguate per promuoverle e potenzialmente integrarle nelle politiche o in altre iniziative. RICONOSCE, a tale proposito, che occorre prestare particolare attenzione all'esame dei vantaggi e degli svantaggi delle soluzioni sistematiche, quali i principi "zero trust", la distinta dei materiali software e analoghe soluzioni a lungo termine. RACCOMANDA di utilizzare a tal fine il gruppo di cooperazione NIS.

25. PRENDE ATTO dei vantaggi offerti dal monitoraggio e da un'efficace condivisione delle informazioni in materia di minacce e incidenti informatici ai fini della prevenzione, dell'individuazione e dell'attenuazione degli effetti degli attacchi alle catene di approvvigionamento. SOTTOLINEA la necessità di continuare a rafforzare la fiducia tra gli Stati membri per un'efficace condivisione di tali informazioni. RICORDA a tale proposito la proposta della Commissione di sostenere gli Stati membri nell'istituzione e nel rafforzamento dei centri operativi di sicurezza (SOC) al fine di creare una rete di SOC in tutta l'UE, per meglio monitorare e anticipare i segnali di attacchi alle reti. RAMMENTA la necessità di complementarità e coordinamento all'interno delle reti e dei meccanismi esistenti e in particolare SOTTOLINEA a tale riguardo il ruolo della rete degli CSIRT e la necessità di esplorare ulteriormente il potenziale di tali reti per promuovere una cultura di condivisione delle informazioni efficiente, sicura e affidabile. RICORDA le iniziative intraprese dagli Stati membri, con il sostegno dell'UE, per istituire CSIRT settoriali, nazionali e regionali e centri di condivisione e analisi delle informazioni (ISAC) nazionali o europei nell'ambito di una rete efficace di partenariati in materia di cibersicurezza nell'Unione.

26. Dato il carattere interconnesso e planetario delle minacce alle catene di approvvigionamento delle TIC, SOTTOLINEA l'importanza di affrontare e rafforzare la sicurezza della catena di approvvigionamento delle TIC a livello mondiale. Alla luce di quanto precede, RACCOMANDA il ricorso a partenariati digitali, dialoghi in materia di cibersicurezza e altre iniziative pertinenti dell'UE, tra cui, se del caso, accordi di libero scambio, per promuovere valutazioni basate sul rischio dei fornitori di prodotti e servizi TIC, il ricorso a fornitori affidabili e l'impiego di un ecosistema digitale sicuro e innovativo basato su norme aperte, interoperabili e trasparenti. RIBADISCE inoltre l'obiettivo dei partenariati Global Gateway e del Consiglio UE-USA per il commercio e la tecnologia, nonché delle attività svolte nell'ambito dei suoi gruppi di lavoro, che consiste nel promuovere il ricorso a fornitori affidabili/non ad alto rischio e sviluppare un meccanismo di finanziamento per consentire progetti che rendano le infrastrutture e i servizi TIC nei paesi terzi più sicuri, resilienti e affidabili, anche astenendosi dal finanziare acquisti da fornitori non affidabili/ad alto rischio in modo tecnologicamente neutro.

27. RIAFFERMA il proprio impegno a contribuire a un ciberspazio aperto, libero, globale, stabile e sicuro, a promuoverlo e a rispettare le norme, le regole e i principi del comportamento responsabile degli Stati nel ciberspazio stabiliti nel quadro delle Nazioni Unite. Per quanto riguarda in particolare la sicurezza della catena di approvvigionamento delle TIC, RICORDA la norma, approvata dal gruppo di esperti governativi e dal gruppo di lavoro aperto delle Nazioni Unite, che incoraggia gli Stati ad adottare misure ragionevoli per garantire l'integrità della catena di approvvigionamento, anche attraverso lo sviluppo di misure di cooperazione obiettive, in modo che gli utenti finali possano avere fiducia nella sicurezza dei prodotti TIC, e ad adoperarsi per prevenire la proliferazione di strumenti e tecniche TIC dolosi e l'uso di funzioni nascoste dannose, e SOSTIENE la sua attuazione su vasta scala.