II

(Atti non legislativi)

RACCOMANDAZIONI

RACCOMANDAZIONE (UE) 2021/1086 DELLA COMMISSIONE
del 23 giugno 2021
sull'istituzione di un'unità congiunta per il ciberspazio

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 292,

considerando quanto segue:

(1) La cibersicurezza è essenziale per un'efficace trasformazione digitale dell'economia e della società. L'UE è impegnata in livelli di investimento senza precedenti per garantire la fiducia dei cittadini, delle imprese e delle autorità pubbliche negli strumenti digitali.

(2) La pandemia di COVID-19 ha accresciuto l'importanza della connettività e della dipendenza dell'Europa da reti e sistemi informatici stabili e ha evidenziato la necessità di proteggere l'intera catena di approvvigionamento. Reti e sistemi informatici affidabili e sicuri sono particolarmente importanti per i soggetti in prima linea nella lotta contro la pandemia, quali ospedali, agenzie mediche e produttori di vaccini. Il coordinamento degli sforzi dell'UE volti a prevenire, individuare, scoraggiare, contrastare, mitigare e rispondere agli attacchi informatici più incisivi contro tali soggetti potrebbe prevenire la perdita di vite umane e i tentativi di compromettere la capacità dell'UE di sconfiggere la pandemia nel modo più rapido possibile. Il rafforzamento della capacità dell'UE di contrastare efficacemente gli attacchi informatici contribuisce inoltre a promuovere un ciberspazio globale, aperto, stabile e sicuro.

(3) Di fronte alla natura transfrontaliera delle minacce alla cibersicurezza e alla continua serie di attacchi sempre più complessi, pervasivi e mirati ([1]), le istituzioni e i soggetti competenti in materia di cibersicurezza dovrebbero potenziare la loro capacità di rispondere a tali minacce e attacchi sfruttando le risorse esistenti e migliorando gli sforzi di coordinamento. Tutti i soggetti interessati nell'UE devono essere pronti a rispondere collettivamente e a scambiarsi informazioni sulla base della «necessità di condividere» piuttosto che della «necessità di sapere».

(4) Nonostante i notevoli progressi compiuti grazie alla cooperazione tra gli Stati membri in materia di cibersicurezza, in particolare attraverso il gruppo di cooperazione («gruppo di cooperazione NIS») e la rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) istituiti a norma della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([2]), non esiste ancora una piattaforma comune dell'UE in cui le informazioni raccolte in diverse comunità di cibersicurezza possano essere scambiate in modo efficiente e sicuro e in cui le capacità operative possano essere coordinate e mobilitate dai soggetti interessati. Le minacce e gli incidenti informatici rischiano pertanto di essere affrontati in compartimenti stagni con un'efficienza limitata e una maggiore vulnerabilità. Manca inoltre un canale a livello di UE per la cooperazione tecnica e operativa con il settore privato, in termini sia di condivisione delle informazioni sia di sostegno per la risposta agli incidenti.

([1]) ENISA, 2020 Threat Landscape; Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020.

([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).

(5) I quadri e le strutture esistenti, così come le risorse e le competenze disponibili negli Stati membri e nelle istituzioni, negli organi e nelle agenzie pertinenti dell'UE, forniscono una solida base per una risposta collettiva alle minacce, agli incidenti e alle crisi di cibersicurezza ([3]). Questa architettura esistente comprende, a livello operativo, il programma per una risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala («il programma») ([4]), la rete di CSIRT e la rete europea delle organizzazioni di collegamento per le crisi informatiche («EU-CyCLONe») ([5]), nonché il Centro europeo per la lotta alla criminalità informatica («EC3») e la task force di azione congiunta contro la criminalità informatica («J-CAT») presso l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto («Europol») e il protocollo di risposta alle emergenze delle autorità di contrasto dell'UE («LE ERP UE»). Il gruppo di cooperazione NIS, il Centro UE di situazione e di intelligence («INTCEN UE»), il pacchetto di strumenti della diplomazia informatica ([6]) e i progetti connessi alla ciberdifesa avviati nell'ambito della cooperazione strutturata permanente (PESCO) ([7]) contribuiscono anch'essi alla cooperazione politica e operativa in diverse comunità di cibersicurezza. L'Agenzia dell'Unione europea per la cibersicurezza («ENISA»), in virtù del suo mandato rafforzato, ha il compito di sostenere la cooperazione operativa ([8]) per quanto riguarda la cibersicurezza delle reti e dei sistemi informatici, gli utenti di tali sistemi e altre persone interessate da minacce e incidenti informatici. Attraverso i dispositivi integrati per la risposta politica alle crisi (IPCR), l'UE è in grado di coordinare la sua risposta politica alle crisi gravi, anche in caso di attacchi informatici su vasta scala.

(6) Tuttavia, non esiste ancora un meccanismo per sfruttare le risorse esistenti e fornire assistenza reciproca tra le comunità informatiche responsabili della sicurezza delle reti e dei sistemi informatici, della lotta alla criminalità informatica, della diplomazia informatica e, se del caso, della ciberdifesa in caso di crisi. Non esiste neppure un meccanismo globale a livello dell'UE per la cooperazione tecnica e operativa tra tutte le comunità in materia di consapevolezza situazionale, preparazione e risposta. Le sinergie con le comunità delle forze dell'ordine e i servizi di intelligence dovrebbero inoltre essere conseguite rispettivamente attraverso Europol e l'INTCEN.

(7) La Commissione, l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (alto rappresentante), gli Stati membri e le istituzioni, gli organi e le agenzie pertinenti dell'UE riconoscono l'importanza di analizzare i punti di forza, le debolezze, le lacune e le sovrapposizioni dell'attuale architettura di cibersicurezza dell'UE creata negli ultimi anni. In consultazione con gli Stati membri, la Commissione, con la partecipazione dell'alto rappresentante, ha elaborato il concetto di unità congiunta per il ciberspazio in risposta a tale analisi e quale componente importante della strategia per l'Unione della sicurezza ([9]), della strategia digitale ([10]) e della strategia per la cibersicurezza ([11]).

([3]) La rete europea delle organizzazioni di collegamento per le crisi informatiche («EU-CyCLONe») è stata istituita dagli Stati membri in risposta alla raccomandazione relativa al programma. La Commissione ha proposto di codificare una rete di esperti nazionali in gestione operativa e delle crisi mediante la direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 [COM (2020) 823 final, 2020/0359 (COD)] proposta nel dicembre 2020.

([4]) Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017, pag. 36).

([5]) La presente raccomandazione tiene conto della relazione successiva all'azione 2020, riguardante l'esercitazione sul livello operativo del programma (Blue OLEx) e, in particolare, della sintesi della presidenza sul dibattito politico e strategico relativo all'unità congiunta per il ciberspazio.

([6]) Conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose («pacchetto di strumenti della diplomazia informatica»), 19 giugno 2017 (9916/17).

([7]) In particolare, i progetti PESCO riguardanti i «gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza» coordinati dalla Lituania e il «Centro di coordinamento nel settore informatico e dell'informazione» coordinato dalla Germania.

([8]) L'articolo 7 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (GU L 151 del 7.6.2019, pag. 15) prevede che l'Agenzia sostenga la cooperazione operativa tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e tra i portatori di interessi. Ciò comprende il sostegno agli Stati membri per quanto riguarda la cooperazione operativa nell'ambito della rete di CSIRT, l'elaborazione periodica di una relazione approfondita sulla situazione tecnica della cibersicurezza nell'UE in merito agli incidenti e alle minacce informatiche e il contributo allo sviluppo di una risposta cooperativa, a livello di Unione e di Stati membri, agli incidenti o alle crisi su vasta scala di carattere transfrontaliero. L'ENISA contribuisce inoltre alle attività di formazione con l'Accademia europea per la sicurezza e la difesa (AESD).

([9]) Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla strategia dell'UE per l'Unione della sicurezza [COM(2020) 605 final].

([10]) Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni — Plasmare il futuro digitale dell'Europa [COM(2020) 67 final].

([11]) Comunicazione congiunta al Parlamento europeo e al Consiglio — La strategia dell'UE in materia di cibersicurezza per il decennio digitale [JOIN(2020) 18 final].

(8) Nei casi di crisi, gli Stati membri dovrebbero poter contare sulla solidarietà dell'UE sotto forma di assistenza coordinata, anche da parte di tutte e quattro le comunità informatiche, ossia le comunità civile, diplomatica, delle forze dell'ordine ([12]) e, se del caso, della difesa. Il grado di intervento dei partecipanti di una o più comunità può dipendere dalla natura dell'incidente o della crisi su vasta scala e, di conseguenza, dal tipo di contromisure necessarie per rispondervi. Di fronte alle minacce, alle crisi e agli incidenti informatici, esperti ben formati e attrezzature tecniche rappresentano elementi essenziali che possono contribuire a evitare danni gravi e consentire una ripresa efficace. Saranno pertanto al centro dell'unità congiunta per il ciberspazio capacità tecniche e operative chiaramente identificate - in primo luogo esperti e attrezzature - pronte per essere mobilitate negli Stati membri in caso di necessità. Nell'ambito di tale piattaforma, i partecipanti si troveranno in una posizione unica per alimentare e coordinare tali capacità attraverso gruppi di reazione rapida dell'UE per la cibersicurezza, garantendo nel contempo adeguate sinergie con i progetti informatici già esistenti attuati nell'ambito della PESCO.

(9) L'unità congiunta per il ciberspazio fornisce una piattaforma virtuale e fisica e non richiede la creazione di un organismo supplementare indipendente. La sua istituzione non dovrebbe pregiudicare le competenze e le facoltà delle autorità nazionali per la cibersicurezza e dei pertinenti organismi dell'Unione. L'unità congiunta per il ciberspazio dovrebbe essere ancorata nei memorandum d'intesa tra i suoi partecipanti. Dovrebbe basarsi sulle strutture, sulle risorse e sulle capacità esistenti e apportarvi un valore aggiunto quale piattaforma per una cooperazione operativa e tecnica, sicura e rapida, tra gli organismi dell'UE e le autorità degli Stati membri. Dovrebbe inoltre riunire tutte le comunità di cibersicurezza, ossia le comunità civile, diplomatica, delle forze dell'ordine e della difesa. I partecipanti alla piattaforma dovrebbero svolgere un ruolo operativo o di sostegno. Tra i partecipanti operativi dovrebbero rientrare l'ENISA, Europol, la squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'UE («CERT-UE»), la Commissione, il servizio europeo per l'azione esterna (compreso l'INTCEN), la rete di CSIRT e l'EU-CyCLONe. I partecipanti sostenitori dovrebbero comprendere l'Agenzia europea per la difesa (AED), il presidente del gruppo di cooperazione NIS, il presidente del gruppo orizzontale del Consiglio per le questioni riguardanti il ciberspazio e un rappresentante dei pertinenti progetti PESCO ([13]). Poiché gli Stati membri dispongono di capacità operative e competenze per rispondere alle minacce, alle crisi e agli incidenti informatici su vasta scala, i partecipanti alla piattaforma dovrebbero basarsi principalmente sulle loro capacità, con l'ausilio dei pertinenti organismi dell'Unione, per conseguire i loro obiettivi.

(10) L'unità congiunta per il ciberspazio dovrebbe imprimere un nuovo slancio al processo avviato nel 2017 con il programma. Dovrebbe rendere ulteriormente operativa l'architettura del programma e segnare una tappa decisiva verso un quadro europeo per la gestione delle crisi di cibersicurezza in cui le minacce e i rischi siano individuati, attenuati e affrontati in modo coordinato e tempestivo. In tal modo l'unità congiunta per il ciberspazio dovrebbe aiutare l'UE a rispondere alle minacce attuali e imminenti.

(11) Partecipando all'unità congiunta per il ciberspazio, i partecipanti operativi e sostenitori dovrebbero poter collaborare con una più ampia gamma di portatori di interessi nell'ambito del quadro di risposta alle crisi di cibersicurezza dell'UE. Nell'esercizio delle loro funzioni entro i limiti dei loro mandati, i partecipanti dovrebbero beneficiare di una maggiore preparazione e di una più ampia consapevolezza situazionale riguardante tutti gli aspetti connessi alle minacce e agli incidenti di cibersicurezza e sfruttare ulteriori competenze in materia di cibersicurezza. Ad esempio, i partecipanti dovrebbero essere regolarmente coinvolti in esercitazioni tra comunità, acquisire un ruolo ben definito nel piano di risposta alle crisi dell'UE, migliorare la visibilità delle loro azioni attraverso una comunicazione pubblica condivisa e concludere accordi di cooperazione operativa con il settore privato. Parallelamente, il contributo all'unità congiunta per il ciberspazio dovrebbe consentire ai partecipanti di rafforzare le reti esistenti, quali la rete di CSIRT e EU-CyCLONe, fornendo loro strumenti sicuri per lo scambio di informazioni e migliori capacità di rilevamento (ad esempio i centri operativi di sicurezza, «SOC») e consentendo loro di sfruttare le capacità operative dell'UE disponibili.

(12) I partecipanti all'unità congiunta per il ciberspazio dovrebbero concentrarsi sulla cooperazione tecnica e operativa, comprese le operazioni congiunte e dovrebbero contribuire a tale cooperazione nella misura consentita dai loro mandati. La cooperazione dovrebbe basarsi sugli sforzi in corso e integrarli. A seconda del tipo di cooperazione in questione, possono intervenire ulteriori partecipanti.

([12]) Rilevante anche per la cooperazione giudiziaria.

([13]) Cfr. nota 5. Il SEAE e l'AED, attraverso il loro ruolo di segretariato della PESCO, collaboreranno con i coordinatori dei pertinenti progetti PESCO.

(13) La piattaforma dovrebbe riunire esperti tecnici e operativi di gestione delle crisi provenienti dagli Stati membri e dagli organismi dell'UE al fine di coordinare le risposte alle minacce, alle crisi e agli incidenti informatici avvalendosi delle capacità e delle competenze esistenti. Gli esperti che partecipano all'unità congiunta per il ciberspazio saranno in grado di monitorare e proteggere una superficie di attacco molto più ampia facendo uso della piattaforma sia fisica che virtuale. A tal fine i partecipanti dovrebbero coordinare gli sforzi in caso di crisi e incidenti transfrontalieri e fornire assistenza ai paesi colpiti dagli incidenti attraverso la piattaforma.

(14) L'istituzione dell'unità congiunta per il ciberspazio impone un processo incrementale che sfrutti e consolidi i quadri e le strutture esistenti menzionati nella presente raccomandazione, compresi i meccanismi di collaborazione istituiti nell'ambito dei consessi guidati dagli Stati membri (ad es. la rete di CSIRT, EU-CyCLONe, il gruppo orizzontale del Consiglio per le questioni riguardanti il ciberspazio, la J-CAT e i progetti PESCO pertinenti) e, dal lato delle istituzioni, degli organi e delle agenzie dell'UE, la cooperazione strutturata ENISA e CERT-UE e il gruppo interistituzionale per lo scambio di informazioni sulla cibersicurezza. Dovrebbero essere opportunamente impiegati i quadri in materia di minacce ibride, di protezione civile ([14]) e settoriali specifici ([15]). Analogamente, dovrebbe essere creato un collegamento strutturato con gli IPCR ([16]). Ciò consentirà, in caso di crisi, di trasmettere rapidamente ed efficacemente ai decisori politici le informazioni raccolte in sede di Consiglio.

(15) La creazione dell'unità congiunta per il ciberspazio dovrebbe pertanto seguire un processo graduale e trasparente da completare nei prossimi due anni. Per questo motivo gli obiettivi stabiliti nella presente raccomandazione dovrebbero essere conseguiti mediante un processo in quattro fasi, come descritto nell'allegato della presente raccomandazione. Nelle prime due fasi dovrebbe essere avviato un processo preparatorio, organizzato e sostenuto dall'ENISA, che coinvolga partecipanti operativi e di sostegno a livello dell'UE e degli Stati membri e si svolga nell'ambito di un gruppo di lavoro che sarà istituito dalla Commissione. I lavori preparatori dovrebbero essere guidati dai principi di impegno reciproco, inclusività e costruzione del consenso. Dovrebbe essere promosso l'impegno di tutti i partecipanti, consentendo di esprimere opinioni e posizioni diverse e cercando di trovare soluzioni che incontrino il più ampio sostegno possibile. In funzione delle esigenze, e sulla base di condizioni ben giustificate, il calendario per le diverse fasi indicate nella presente raccomandazione può essere adeguato.

(16) Nella prima fase il processo preparatorio dovrebbe iniziare con l'individuazione delle pertinenti capacità operative disponibili dell'UE e con l'avvio di una valutazione dei ruoli e delle responsabilità dei partecipanti all'interno della piattaforma. La seconda fase dovrebbe comprendere lo sviluppo del piano dell'UE di risposta agli incidenti e alle crisi, in linea con il programma ([17]), l'avvio di attività connesse alla preparazione e alla consapevolezza situazionale, in linea con il regolamento sulla cibersicurezza e con il regolamento Europol ([18]), e la conclusione della valutazione dei ruoli e delle responsabilità dei partecipanti all'interno della piattaforma. Il gruppo di lavoro dovrebbe presentare i risultati di tale valutazione alla Commissione e all'alto rappresentante, che successivamente condivideranno tali risultati con il Consiglio. La Commissione e l'alto rappresentante dovrebbero collaborare, secondo le rispettive competenze, per elaborare una relazione congiunta sulla base di tale valutazione e invitare il Consiglio ad approvarla mediante conclusioni del Consiglio.

(17) A seguito di tale approvazione l'unità congiunta per il ciberspazio sarà resa operativa nell'ottica di completare le due fasi restanti del processo. Nella terza fase i partecipanti dovrebbero essere in grado di mobilitare i gruppi di reazione rapida dell'UE nell'ambito dell'unità congiunta per il ciberspazio, in base a procedure definite nel piano dell'UE di risposta agli incidenti e alle crisi, facendo leva sulla piattaforma sia fisica che virtuale e contribuendo a vari aspetti della risposta agli incidenti (dalla comunicazione pubblica al recupero ex post). Nella quarta fase, infine, i portatori di interessi del settore privato, compresi gli utenti e i fornitori di soluzioni e servizi di cibersicurezza, saranno invitati a offrire il proprio contributo alla piattaforma, consentendo ai partecipanti di migliorare la condivisione delle informazioni e potenziare la risposta coordinata dell'UE alle minacce e agli incidenti informatici.

([14]) In tale contesto l'unità congiunta per il ciberspazio dovrebbe creare sinergie con il meccanismo unionale di protezione civile (UCPM) per potenziare la preparazione e la risposta a livello europeo in caso di catastrofi multiple ed emergenze che includono un elemento informatico.

([15]) Come il quadro per il settore finanziario previsto dal regolamento (UE) 2021/xx del Parlamento europeo e del Consiglio* [DORA].

([16]) Cfr. considerando 5.

([17]) Cfr. nota 3.

([18]) Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI (GU L 135 del 24.5.2016, pag. 53).

(18) Entro la fine delle quattro fasi del processo, i partecipanti dovrebbero elaborare una relazione di attività sui progressi compiuti nell'attuazione delle quattro fasi indicate nella raccomandazione, che descriva i risultati conseguiti e le sfide da affrontare e che dovrebbe essere presentata alla Commissione e all'alto rappresentante. Sulla base di tale relazione la Commissione e l'alto rappresentante dovrebbero effettuare una valutazione di tali risultati e trarre conclusioni per il futuro dell'unità congiunta per il ciberspazio.

(19) La Commissione, l'ENISA, Europol e il CERT-UE dovrebbero fornire sostegno amministrativo, finanziario e tecnico all'unità congiunta per il ciberspazio come indicato alla sezione IV della presente raccomandazione, subordinatamente alla disponibilità di bilancio e di risorse umane. Il rafforzamento delle capacità operative di cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE pertinenti sarà fondamentale per garantire una preparazione efficace e la sostenibilità dell'unità congiunta per il ciberspazio. La Commissione intende garantire che il prossimo regolamento recante norme comuni vincolanti in materia di cibersicurezza per le istituzioni, gli organi e le agenzie dell'UE (ottobre 2021) fornisca la base giuridica per tale contributo nel caso del CERT-UE.

(20) Visto il suo mandato rafforzato a norma del regolamento (UE) 2019/881 («regolamento sulla cibersicurezza»), l'ENISA si trova in una posizione unica per organizzare e sostenere la preparazione dell'unità congiunta per il ciberspazio e per contribuire alla sua operatività. In linea con le disposizioni del regolamento sulla cibersicurezza, l'ENISA sta attualmente predisponendo un ufficio a Bruxelles a supporto della sua cooperazione strutturata con il CERT-UE. Tale cooperazione strutturata, compresi gli uffici adiacenti, fornisce un quadro utile per agevolare la creazione dell'unità congiunta per il ciberspazio, inclusa la delimitazione del suo spazio fisico che dovrebbe essere messo a disposizione dei partecipanti in caso di necessità, nonché del personale di altre istituzioni, organi e agenzie pertinenti dell'UE. La piattaforma fisica dovrebbe essere abbinata a una piattaforma virtuale composta da strumenti collaborativi e sicuri per la condivisione delle informazioni. Tali strumenti si baseranno sulle molteplici informazioni raccolte attraverso il Cyber-Shield europeo ([19]), compresi i centri operativi per la sicurezza («SOC») e i centri di condivisione e analisi delle informazioni («ISAC»).

(21) Il protocollo di risposta alle emergenze delle autorità di contrasto dell'UE criminalità informatica per i gravi attacchi informatici transfrontalieri, adottato dal Consiglio nel 2018, attribuisce un ruolo centrale al Centro europeo per la lotta alla criminalità informatica di Europol («EC3») ([20]) nell'ambito del programma. Tale protocollo consente alle autorità di contrasto dell'UE di rispondere agli attacchi transfrontalieri su vasta scala di sospetta natura dolosa su base 24/7 attraverso una reazione e una valutazione rapide; esso permette inoltre la condivisione sicura e tempestiva di informazioni critiche per un coordinamento efficace delle risposte agli incidenti transfrontalieri. Il protocollo dettaglia ulteriormente la collaborazione con altre istituzioni dell'UE, i protocolli di crisi a livello dell'UE e la cooperazione con il settore privato in caso di crisi. La comunità delle autorità di contrasto, con il sostegno di Europol ove opportuno, dovrebbe contribuire all'unità congiunta per il ciberspazio adottando i provvedimenti necessari lungo tutto l'arco del ciclo investigativo, in linea con i requisiti del quadro di giustizia penale e le procedure applicabili per il trattamento delle prove elettroniche. Dall'avvio dell'EC3 nel 2013, Europol fornisce sostegno operativo e agevola la cooperazione operativa contro le minacce informatiche. Europol dovrebbe sostenere la piattaforma in conformità al suo mandato e all'approccio di polizia basato sull'intelligence, sfruttando nel contempo tutti i tipi di competenze, prodotti, strumenti e servizi interni pertinenti per la risposta all'incidente o alla crisi.

(22) La direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione impone inoltre agli Stati membri di predisporre un punto di contatto operativo nazionale disponibile ventiquattr'ore su ventiquattro e sette giorni su sette, per lo scambio di informazioni relative ai reati di cui a tale direttiva. La rete dei punti di contatto operativi nazionali dovrebbe inoltre contribuire all'unità congiunta per il ciberspazio garantendo, se del caso, il coinvolgimento delle autorità di contrasto degli Stati membri.

(23) La comunità della diplomazia informatica dell'UE contribuisce a promuovere e proteggere un ciberspazio globale, aperto, stabile e sicuro e a prevenire, scoraggiare e rispondere a tali attività informatiche dolose. Nel 2017 l'UE ha istituito un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose («pacchetto di strumenti della diplomazia informatica»). Questo quadro fa parte della più ampia politica dell'UE in materia di diplomazia informatica e contribuisce alla prevenzione dei conflitti e a una maggiore stabilità nelle relazioni internazionali. Consente all'UE e agli Stati membri, in cooperazione con i partner internazionali ove opportuno, di utilizzare tutte le misure della politica estera e di sicurezza comune («PESC»), in linea con le rispettive procedure per il loro conseguimento, per incoraggiare la cooperazione, attenuare le minacce e influenzare i comportamenti dolosi attuali e potenziali futuri nel ciberspazio. La comunità della diplomazia informatica dovrebbe cooperare nell'ambito dell'unità congiunta per il ciberspazio utilizzando l'intera gamma di misure diplomatiche e fornendo sostegno nell'utilizzo di tali misure, in particolare per quanto riguarda la comunicazione pubblica, e sostenendo la consapevolezza situazionale condivisa e l'impegno con i paesi terzi in caso di crisi.

([19]) JOIN/2020/18 final, sezione 1.2.
([20]) Stabilito con il regolamento (UE) 2016/794.

(24) In linea con il quadro del programma, l'alto rappresentante, anche attraverso l'INTCEN, dovrebbe contribuire all'unità congiunta per il ciberspazio fornendo una continua consapevolezza situazionale condivisa, basata sull'intelligence, sulle minacce esistenti ed emergenti, compresa la necessaria consapevolezza situazionale strategica per ciascun evento.

(25) All'interno della comunità della ciberdifesa, l'UE e gli Stati membri mirano a rafforzare le capacità di ciberdifesa e a potenziare ulteriormente le sinergie, il coordinamento e la cooperazione tra le istituzioni, gli organi e le agenzie competenti dell'UE, nonché con e tra gli Stati membri, anche per quanto riguarda le missioni e le operazioni nell'ambito della politica di sicurezza e di difesa comune («PSDC»). La comunità opera sulla base di una governance intergovernativa a livello dell'UE, di strutture di comando militari nazionali e di capacità e mezzi militari o a duplice uso. Alla luce della sua diversa natura, dovrebbero essere costruite interfacce specifiche con l'unità congiunta per il ciberspazio per consentire la condivisione delle informazioni con la comunità della ciberdifesa ([21]).

(26) La cooperazione strutturata permanente è un quadro giuridico introdotto dal trattato di Lisbona ([22]) e istituito nel 2017 nell'ambito dell'Unione. La cooperazione strutturata ha portato alla definizione di una serie di progetti PESCO nel settore informatico, che contribuiscono alla realizzazione dell'impegno 11 ([23]) di «aumentare gli sforzi nella cooperazione in materia di ciberdifesa, ad esempio attraverso la condivisione delle informazioni, la formazione e il supporto operativo». Il SEAE, insieme allo Stato maggiore dell'UE e l'EDA, fa parte del segretariato della PESCO, che costituisce un punto di contatto unico nel quadro dell'Unione per tutte le questioni relative alla PESCO, comprese le funzioni di sostegno e coordinamento connesse ai progetti PESCO (ad esempio la valutazione di nuove proposte di progetti, la preparazione delle relazioni sullo stato di avanzamento dei progetti ecc.). I rappresentanti dei pertinenti progetti PESCO dovrebbero sostenere l'unità congiunta per il ciberspazio, in particolare per quanto riguarda la consapevolezza situazionale e la preparazione.

(27) Attraverso l'unità congiunta per il ciberspazio, i partecipanti dovrebbero integrare adeguatamente i portatori di interessi del settore privato, compresi i fornitori e gli utenti di soluzioni e servizi di cibersicurezza, al fine di sostenere il quadro europeo di gestione delle crisi di cibersicurezza, tenendo in debita considerazione il quadro giuridico per la condivisione dei dati e la sicurezza dell'informazione. I fornitori di cibersicurezza dovrebbero contribuire all'iniziativa condividendo informazioni sulle minacce e mettendo a disposizione addetti alla gestione degli incidenti per ampliare rapidamente la capacità dell'unità di rispondere ad attacchi e crisi su vasta scala. Gli utenti di beni e servizi di cibersicurezza, principalmente quelli che rientrano nell'ambito di applicazione della direttiva NIS, dovrebbero poter chiedere aiuto e consulenza attraverso canali strutturati, che attualmente mancano, collegati ai centri di condivisione e analisi delle informazioni (ISAC) a livello dell'UE ([24]). La piattaforma potrebbe inoltre contribuire a rafforzare la cooperazione con partner internazionali.

(28) Lo sviluppo e il mantenimento della consapevolezza situazionale richiedono capacità di rilevamento e di prevenzione delle intrusioni all'avanguardia. L'unità congiunta per il ciberspazio dovrebbe basarsi su una rete di punta in grado di analizzare le minacce e gli incidenti dolosi che possono avere un impatto sui principali sistemi di comunicazione e informazione in tutta l'Unione. Ciò significa che, tra le altre fonti, la conoscenza sulle minacce tratta dalle reti di comunicazione monitorate dai SOC nazionali, settoriali e transfrontalieri dovrebbe confluire nell'unità congiunta per il ciberspazio per migliorare la valutazione dei partecipanti in merito al panorama delle minacce dell'UE

(29) Al fine di sostenere lo scambio di informazioni operative, eventualmente anche di materiale riservato, la piattaforma dovrebbe basarsi su canali di comunicazione adeguatamente protetti. Tali canali potrebbero anche basarsi sull'infrastruttura esistente, come l'applicazione di rete per lo scambio di informazioni protetta («SIENA») utilizzata da Europol e dalle autorità di contrasto. Come annunciato nella strategia per la cibersicurezza, gli strumenti utilizzati dalle istituzioni, dagli organi e dalle agenzie dell'UE dovrebbero rispettare le norme sulla sicurezza delle informazioni che la Commissione proporrà a breve.

([21]) In particolare attraverso la rappresentanza del SEAE, al fine di consentire l'opportuno coinvolgimento della comunità della ciberdifesa, che si basa sui contributi nazionali volontari.

([22]) Articolo 42, paragrafo 6, articolo 46 e protocollo 10, TUE.

([23]) Ciascuno degli Stati membri partecipanti alla PESCO assume 20 impegni specifici, suddivisi nei cinque settori chiave di cui all'articolo 2 del protocollo n. 10 sulla PESCO allegato al trattato sull'Unione europea.

([24]) Esempi significativi di ISAC esistenti che potrebbero essere coinvolti in tale condivisione sono l'ISAC europeo dell'energia (EE-ISAC) o l'ISAC degli istituti finanziari europei (FI-ISAC).

(30) La Commissione, principalmente attraverso il programma Europa digitale, sosterrà gli investimenti necessari per istituire la piattaforma fisica e virtuale, costruire e mantenere canali di comunicazione e capacità di formazione sicuri e sviluppare e mobilitare capacità di rilevamento. In aggiunta, il Fondo europeo per la difesa potrebbe contribuire a finanziare tecnologie e capacità di ciberdifesa fondamentali che rafforzerebbero la preparazione nazionale in materia di ciberdifesa,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

I. **SCOPO DELLA PRESENTE RACCOMANDAZIONE**

1) Lo scopo della presente raccomandazione è individuare le azioni necessarie per coordinare gli sforzi dell'UE volti a prevenire, rilevare, scoraggiare, contrastare e attenuare le crisi e gli incidenti informatici su vasta scala e rispondervi attraverso un'unità congiunta per il ciberspazio. A tal fine la presente raccomandazione definisce inoltre il processo, le tappe e il calendario che gli Stati membri e le istituzioni, gli organi e le agenzie pertinenti dell'UE dovrebbero adottare in relazione alla creazione e allo sviluppo di tale piattaforma.

2) In caso di incidenti e crisi di cibersicurezza su vasta scala gli Stati membri e le istituzioni, gli organi e le agenzie pertinenti dell'UE dovrebbero garantire il coordinamento dei loro sforzi attraverso un'unità congiunta per il ciberspazio che consenta l'assistenza reciproca ([25]) sfruttando le competenze delle autorità degli Stati membri e delle istituzioni, degli organi e delle agenzie pertinenti dell'UE. L'unità congiunta per il ciberspazio dovrebbe inoltre consentire ai partecipanti di collaborare con il settore privato.

II. **DEFINIZIONI**

3) Ai fini della presente raccomandazione si applicano le definizioni seguenti:

a) «piano dell'UE di risposta agli incidenti e alle crisi di cibersicurezza»: una raccolta di ruoli, modalità e procedure volti al completamento del quadro di risposta alle crisi di cibersicurezza dell'UE di cui al punto 1) della raccomandazione della Commissione del 13 settembre 2017 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala («programma»);

b) «comunità di cibersicurezza»: gruppi di collaborazione civili, diplomatici, delle forze dell'ordine e della difesa che rappresentano sia gli Stati membri sia le istituzioni, gli organi e le agenzie pertinenti dell'UE che si scambiano informazioni per perseguire obiettivi, interessi e missioni comuni in relazione alla cibersicurezza;

c) «partecipanti del settore privato»: rappresentanti di soggetti del settore privato che forniscono o utilizzano soluzioni ([26]) e servizi di cibersicurezza ([27]);

d) «incidente su vasta scala»: un incidente quale definito all'articolo 4, punto 7, della direttiva (UE) 2016/1148 con un impatto significativo in almeno due Stati membri;

e) «relazione integrata sulla situazione della cibersicurezza nell'UE»: una relazione che riunisce i contributi dei partecipanti all'unità congiunta per il ciberspazio, sulla base della relazione sulla situazione tecnica della cibersicurezza nell'Unione di cui all'articolo 7, paragrafo 6, del regolamento (UE) 2019/881;

f) «gruppo di reazione rapida dell'UE per la cibersicurezza»: un gruppo composto da esperti riconosciuti in materia di cibersicurezza, provenienti in particolare dai CSIRT degli Stati membri, con il sostegno dell'ENISA, del CERT-UE e di Europol, pronto ad assistere a distanza i partecipanti colpiti da incidenti e crisi su vasta scala;

g) «memorandum d'intesa»: un accordo tra i partecipanti che stabilisce le necessarie modalità di cooperazione, compresa la definizione delle risorse e delle procedure necessarie per istituire e mobilitare i gruppi di reazione rapida dell'UE per la cibersicurezza, nonché per consentire l'assistenza reciproca.

([25]) Coerentemente con l'approccio e i principi di cui alla direttiva (UE) 2016/1148 e all'articolo 222 TFUE. Fatto salvo l'articolo 42, paragrafo 7, del trattato sull'Unione europea.
([26]) Compresi i fornitori di software.
([27]) Compresa l'intelligence sulle minacce.

III. **OBIETTIVO DELL'UNITÀ CONGIUNTA PER IL CIBERSPAZIO**

4) Gli Stati membri e le istituzioni, gli organi e le agenzie pertinenti dell'UE dovrebbero garantire **una risposta coordinata dell'UE** alle crisi e agli incidenti informatici su vasta scala e la ripresa dagli stessi. Tale risposta dovrebbe in particolare essere garantita tra i partecipanti operativi, in particolare ENISA, Europol, CERT-UE, Commissione, servizio europeo per l'azione esterna (compreso l'INTCEN), rete di CSIRT, EU-CyCLONe, e i partecipanti sostenitori, in particolare il presidente del gruppo di cooperazione NIS, il presidente del gruppo orizzontale del Consiglio per le questioni riguardanti il ciberspazio, l'Agenzia europea per la difesa e un rappresentante dei pertinenti progetti PESCO ([28]). I partecipanti operativi dovrebbero essere in grado di mobilitare rapidamente ed efficacemente risorse operative per l'assistenza reciproca nell'ambito dell'unità congiunta per il ciberspazio. A tal fine, nell'ambito dell'unità congiunta per il ciberspazio, i meccanismi di assistenza reciproca dovrebbero essere coordinati su richiesta di uno o più Stati membri.

5) Al fine di fornire una risposta coordinata efficace, i partecipanti operativi e i partecipanti sostenitori elencati al punto 4) dovrebbero essere in grado di condividere le migliori pratiche, sfruttare una costante **consapevolezza situazionale condivisa** e garantire la **preparazione** necessaria nella misura consentita dai loro mandati. Tali partecipanti dovrebbero tenere conto dei processi esistenti e delle competenze delle diverse comunità di cibersicurezza.

IV. **DEFINIZIONE DEL FUNZIONAMENTO DELL'UNITÀ CONGIUNTA PER IL CIBERSPAZIO**

6) Gli Stati membri e le istituzioni, gli organi e le agenzie pertinenti dell'UE, basandosi sul contributo dell'ENISA in conformità all'articolo 7, paragrafo 7, del regolamento (UE) 2019/881, dovrebbero garantire una **risposta coordinata** agli incidenti e alle crisi su vasta scala e una ripresa dagli stessi mediante:

a) l'istituzione, la formazione, la verifica e la mobilitazione coordinata di **gruppi di reazione rapida dell'UE per la cibersicurezza**, basandosi su quanto stabilito all'articolo 7, paragrafo 4, del regolamento (UE) 2019/881 e agli articoli 3 e 4 del regolamento (UE) 2016/794;

b) la realizzazione coordinata di una **piattaforma virtuale e fisica**, basandosi sulla cooperazione strutturata di ENISA e CERT-UE sancita dall'articolo 7, paragrafo 4, del regolamento (UE) 2019/881, che dovrebbe fungere da infrastruttura di supporto per la cooperazione tecnica e operativa tra i partecipanti e per riunire personale e altre risorse pertinenti dei partecipanti;

c) la creazione e il mantenimento di un inventario delle **capacità tecniche e operative disponibili nell'UE** in tutte le comunità di cibersicurezza ([29]) dell'Unione, pronte per essere mobilitate in caso di incidenti o crisi di cibersicurezza su vasta scala;

d) la presentazione di relazioni alla Commissione e all'alto rappresentante in merito all'esperienza acquisita nelle attività di **cooperazione operativa in materia di cibersicurezza** all'interno delle comunità di cibersicurezza e tra queste ultime.

7) Gli Stati membri e le istituzioni, gli organi e le agenzie pertinenti dell'UE dovrebbero garantire che l'unità congiunta per il ciberspazio provveda a una costante **consapevolezza situazionale** condivisa e alla **preparazione** alle crisi favorite dall'informatica tra le comunità di cibersicurezza, nonché all'interno di tali comunità, perseguendo gli obiettivi di cui all'articolo 7 del regolamento (UE) 2019/881 e all'articolo 3 del regolamento (UE) 2016/794. A tal fine, gli Stati membri e le istituzioni, gli organi e le agenzie pertinenti dell'UE, in conformità al regolamento (UE) 2019/881 e al regolamento (UE) 2016/794, dovrebbero consentire l'attuazione delle seguenti operazioni **di sostegno**:

a) l'elaborazione della **relazione integrata sulla situazione della cibersicurezza nell'UE** attraverso la raccolta e l'analisi di tutte le informazioni e l'intelligence sulle minacce pertinenti;

b) l'uso di **strumenti** adeguati e sicuri, in linea con l'articolo 7, paragrafo 1, del regolamento (UE) 2019/881, per uno scambio rapido di informazioni tra i partecipanti e con altri soggetti;

c) lo **scambio delle informazioni e delle competenze** necessarie per preparare l'Unione a gestire le crisi e gli incidenti su larga scala favoriti dall'informatica, con il sostegno dell'ENISA, come stabilito all'articolo 7, paragrafo 2, del regolamento (UE) 2019/881;

d) l'adozione e la verifica dei **piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza** ([30]) conformemente all'articolo 7, paragrafi 2, 5 e 7 del regolamento (UE) 2019/881;

([28]) «Centro di coordinamento nel settore informatico e dell'informazione» (CIDCC) e «gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza» (CRRT).

([29]) Compresa, se del caso, la comunità di ciberdifesa.

([30]) Proposto in base all'articolo 7, paragrafo 3, della direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (COM(2020) 823 final, 2020/0359 (COD)).

e) lo sviluppo, la gestione e la verifica, anche attraverso esercitazioni e formazioni tra comunità, del **piano dell'UE di risposta agli incidenti e alle crisi di cibersicurezza**, in conformità alla raccomandazione sul «programma» e sulla base dell'articolo 7, paragrafo 3, della proposta della Commissione di revisione della direttiva (UE) 2016/1148 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione ([31]);

f) l'assistenza dei partecipanti nella conclusione di accordi per lo scambio di informazioni, nonché di accordi di cooperazione operativa con **soggetti del settore privato** che forniscono, tra l'altro, intelligence sulle minacce e servizi di risposta agli incidenti, con il sostegno dell'ENISA come stabilito all'articolo 7, paragrafo 1, del regolamento (UE) 2019/881;

g) l'istituzione di sinergie strutturate con **capacità di monitoraggio e rilevamento** nazionali, settoriali e transfrontaliere, in particolare con i centri operativi di sicurezza;

h) l'assistenza dei partecipanti nella **gestione** di crisi e incidenti su vasta scala, in linea con il ruolo di sostegno dell'ENISA stabilito all'articolo 7 del regolamento (UE) 2019/881. Ciò comprende il contributo alla consapevolezza situazionale condivisa, il sostegno all'azione diplomatica, l'attribuzione politica e l'attribuzione nel contesto delle indagini penali, anche attraverso Europol ([32]), l'allineamento della comunicazione pubblica e l'agevolazione della ripresa dagli incidenti.

8) Al fine di attuare i punti 6) e 7), gli Stati membri e le istituzioni, gli organi e le agenzie pertinenti dell'UE dovrebbero garantire:

a) la definizione degli aspetti organizzativi dell'unità congiunta per il ciberspazio e **dei ruoli e delle responsabilità** dei partecipanti operativi e dei partecipanti sostenitori all'interno della piattaforma, consentendo l'efficace funzionamento della piattaforma in linea con gli aspetti e i principi specificati nell'allegato della presente raccomandazione;

b) la conclusione di **memorandum d'intesa** che stabiliscono le necessarie modalità di cooperazione tra i partecipanti di cui al punto 4).

9) In conformità all'articolo 7 del regolamento (UE) 2019/881, l'ENISA dovrebbe garantire il coordinamento degli Stati membri e delle istituzioni, degli organi e delle agenzie pertinenti dell'UE e il sostegno agli stessi all'interno dell'unità congiunta per il ciberspazio, anche svolgendo compiti di segretariato, organizzando riunioni e contribuendo all'attuazione delle azioni a livello sia degli Stati membri sia dell'UE. L'ENISA dovrebbe istituire sia una piattaforma virtuale sicura sia uno spazio fisico per ospitare le riunioni e agevolare le necessarie azioni di attuazione.

V. ISTITUZIONE DELL'UNITÀ CONGIUNTA PER IL CIBERSPAZIO

10) Gli Stati membri e le istituzioni, gli organismi e le agenzie pertinenti dell'UE dovrebbero garantire che l'unità congiunta per il ciberspazio avvii la fase operativa a decorrere dal **30 giugno 2022**. Entro tale data, i partecipanti operativi dovrebbero mettere a disposizione capacità operative ed esperti che possano costituire la base dei gruppi di reazione rapida dell'UE per la cibersicurezza. I piani per una piattaforma fisica e virtuale dovrebbero essere in fase avanzata.

11) Gli Stati membri e le istituzioni, gli organismi e le agenzie pertinenti dell'UE dovrebbero contribuire al funzionamento dell'unità congiunta per il ciberspazio e garantire che sia pienamente operativa entro il **30 giugno 2023**. Questo obiettivo dovrebbe essere conseguito attraverso quattro fasi successive, volte a completare le seguenti attività:

a) fase uno — Valutare gli aspetti organizzativi dell'unità congiunta per il ciberspazio e individuare le capacità operative disponibili dell'UE entro il **31 dicembre 2021**;

b) fase due — Preparare piani di risposta agli incidenti e alle crisi e avviare le attività congiunte di preparazione entro il **30 giugno 2022**;

c) fase tre — Rendere operativa l'unità congiunta per il ciberspazio entro il **31 dicembre 2022**;

d) fase quattro — Estendere la cooperazione nell'ambito dell'unità congiunta per il ciberspazio a soggetti privati e riferire sui progressi compiuti entro il **30 giugno 2023**.

Una descrizione più dettagliata delle azioni da intraprendere nell'ambito delle quattro fasi successive figura nell'allegato della presente raccomandazione.

([31]) COM(2020) 823 final.
([32]) In linea con il regolamento (UE) 2016/794.

12) Nelle prime due fasi l'ENISA dovrebbe organizzare e sostenere la preparazione dell'unità congiunta per il ciberspazio. I servizi della Commissione dovrebbero convocare un gruppo di lavoro che riunisce i partecipanti operativi e i partecipanti sostenitori per portare a termine tali lavori preparatori. I servizi della Commissione dovrebbero nominare un rappresentante come copresidente del gruppo di lavoro e invitare a fungere da copresidenti un rappresentante designato dall'alto rappresentante (ciascuno contribuisce ai punti all'ordine del giorno secondo le rispettive competenze) e un rappresentante scelto dagli Stati membri.

13) Entro la fine della fase due, il gruppo di lavoro dovrebbe concludere la propria valutazione degli aspetti organizzativi dell'unità congiunta per il ciberspazio e dei ruoli e delle responsabilità dei partecipanti operativi all'interno di tale piattaforma. Il gruppo di lavoro dovrebbe presentare i risultati di tale valutazione alla Commissione e all'alto rappresentante. La Commissione e l'alto rappresentante dovrebbero a loro volta condividere detta valutazione con il Consiglio. La Commissione e l'alto rappresentante dovrebbero elaborare una relazione congiunta sulla base di tale valutazione e invitare il Consiglio ad approvarla mediante conclusioni del Consiglio.

14) L'unità congiunta per il ciberspazio dovrebbe essere operativa a partire dalla terza fase.

15) L'ENISA e la Commissione dovrebbero garantire l'uso delle risorse esistenti nell'ambito dei programmi di finanziamento dell'UE, in primo luogo il programma Europa digitale, in linea con le norme applicabili per stabilire i rispettivi programmi di lavoro, per dotare i partecipanti all'unità congiunta per il ciberspazio di ulteriori capacità di formazione, capacità di comunicazione e infrastrutture sicure per la condivisione delle informazioni che consentano lo scambio di informazioni classificate anche tra comunità.

VI. **RIESAME**

16) Gli Stati membri dovrebbero cooperare con la Commissione e l'alto rappresentante, in linea con le rispettive competenze, per valutare l'efficacia e l'efficienza dell'unità congiunta per il ciberspazio entro il **30 giugno 2025**, al fine di trarre conclusioni per il futuro dell'unità congiunta per il ciberspazio. Tale valutazione dovrebbe tenere conto dell'attuazione delle quattro fasi summenzionate.

Fatto a Bruxelles, il 23 giugno 2021

Per la Commissione
Thierry BRETON
Membro della Commissione

ALLEGATO

Fasi dell'istituzione dell'unità congiunta per il ciberspazio

Il presente allegato descrive in maggiore dettaglio le azioni principali e quelle di sostegno necessarie per istituire e rendere operativa l'unità congiunta per il ciberspazio.

1. *Fase 1 — Valutare gli aspetti organizzativi dell'unità congiunta per il ciberspazio e individuare le capacità operative disponibili dell'UE*

AZIONI PRINCIPALI

I partecipanti operativi dell'unità congiunta per il ciberspazio, riuniti in un gruppo di lavoro istituito dalla Commissione e con il sostegno dell'ENISA, dovrebbero raccogliere informazioni sulle capacità operative esistenti, compreso un elenco dei professionisti riconosciuti disponibili con l'indicazione delle loro competenze pertinenti, degli strumenti, delle funzioni e delle risorse disponibili per il trattamento degli incidenti, dei portafogli di formazione ed esercitazione disponibili e dei prodotti esistenti per l'analisi delle informazioni e dell'intelligence. Sulla base di tali informazioni i partecipanti operativi dovrebbero preparare un **elenco delle capacità operative disponibili dell'UE** pronte ad essere mobilitate in caso di incidenti o crisi informatici, in particolare attraverso i gruppi di reazione rapida dell'UE per la cibersicurezza.

Il gruppo di lavoro dovrebbe avviare una valutazione degli **aspetti organizzativi** dell'unità congiunta per il ciberspazio e **dei ruoli e delle responsabilità dei partecipanti operativi all'interno della piattaforma**.

Al fine di acquisire una visione d'insieme delle capacità e concordare le procedure, le azioni principali e, nella misura del possibile, quelle di sostegno della fase uno dovrebbero essere completate **entro il 31 dicembre 2021 [6 mesi dopo l'adozione]**.

2. *Fase 2 — Preparare piani di risposta agli incidenti e alle crisi e avviare le attività congiunte di preparazione*

AZIONI PRINCIPALI

I partecipanti operativi del gruppo di lavoro, in consultazione con i partecipanti di sostegno, dovrebbero preparare il **piano dell'UE di risposta agli incidenti e alle crisi di cibersicurezza** sulla base dei piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza. Il piano dell'UE di risposta agli incidenti e alle crisi di cibersicurezza dovrebbe comprendere gli obiettivi di preparazione dell'UE, le procedure e i canali sicuri individuati per la condivisione di informazioni, comprese le modalità di gestione delle informazioni, e i criteri di attivazione del meccanismo di assistenza reciproca sulla base di una tassonomia concordata di classificazione degli incidenti e dell'elenco delle capacità disponibili dell'UE.

Entro la fine della fase due, il gruppo di lavoro dovrebbe concludere la propria valutazione degli aspetti organizzativi dell'unità congiunta per il ciberspazio e dei ruoli e delle responsabilità dei partecipanti operativi all'interno di tale piattaforma. Il gruppo di lavoro dovrebbe presentare i risultati di tale valutazione alla Commissione e all'alto rappresentante. La Commissione e l'alto rappresentante dovrebbero condividere tale valutazione con il Consiglio. La Commissione e l'alto rappresentante dovrebbero collaborare, secondo le rispettive competenze, per elaborare una relazione congiunta sulla base di tale valutazione e invitare il Consiglio ad approvarla mediante conclusioni del Consiglio.

AZIONI DI SOSTEGNO

Il piano dell'UE di risposta agli incidenti e alle crisi di cibersicurezza dovrebbe basarsi sui principali elementi dei piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza. In linea con la proposta della Commissione di una direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 ([1]), gli Stati membri dovrebbero adottare piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza. I piani nazionali, eventualmente oggetto di valutazione inter pares, dovrebbero definire gli obiettivi e le modalità di gestione degli incidenti e delle crisi di cibersicurezza su vasta scala. I piani nazionali dovrebbero contemplare, in particolare, i seguenti aspetti:

a) gli obiettivi delle misure e delle attività nazionali di preparazione;

b) i compiti e le responsabilità delle autorità nazionali competenti a livello nazionale;

c) le procedure nazionali di gestione delle crisi e i canali nazionali di scambio delle informazioni;

d) l'individuazione delle misure di preparazione, comprese le esercitazioni e le attività di formazione;

e) l'individuazione dei pertinenti portatori di interessi pubblici e privati e delle infrastrutture coinvolte;

f) le procedure nazionali e gli accordi tra le autorità e gli organismi nazionali pertinenti, compresi quelli responsabili di tutte le comunità informatiche, per garantire l'effettiva partecipazione degli Stati membri e il loro sostegno alla gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala a livello dell'UE.

Sulla base dei contributi forniti dagli Stati membri e dalle istituzioni, dagli organismi e dalle agenzie dell'UE, i partecipanti operativi dovrebbero attuare le seguenti azioni di sostegno nel quadro dell'unità congiunta per il ciberspazio:

a) redigere la prima relazione integrata sulla situazione nell'UE, sulla base dei piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza;

([1]) COM(2020) 823 final, 2020/0359 (COD), Bruxelles, 16.12.2020.

b) istituire capacità di comunicazione e strumenti sicuri per la condivisione delle informazioni;

c) facilitare l'adozione di protocolli di assistenza reciproca tra i partecipanti;

d) organizzare esercitazioni e formazioni tra comunità rivolte agli esperti inclusi nell'elenco delle capacità operative disponibili dell'UE;

e) elaborare un piano pluriennale di coordinamento delle esercitazioni.

Qualora necessario i partecipanti operativi dovrebbero consultare i partecipanti di sostegno. L'ENISA, con il sostegno della Commissione, di Europol e del CERT-UE, dovrebbe rendere possibile la condivisione delle informazioni istituendo capacità di comunicazione e strumenti sicuri per la condivisione delle informazioni.

Per garantire la definizione dei piani necessari e l'avvio delle attività congiunte, le azioni principali e, nella misura del possibile, quelle di sostegno della fase due dovrebbero essere completate **entro il 30 giugno 2022 [6 mesi dopo la fine della fase 1]**.

3. *Fase 3 — Rendere operativa l'unità congiunta per il ciberspazio*

AZIONI PRINCIPALI

Successivamente all'approvazione da parte del Consiglio delle conclusioni della Commissione sulla relazione di cui alla fase due, i partecipanti operativi dovrebbero coordinare la mobilitazione dei **gruppi di reazione rapida dell'UE per la cibersicurezza** all'interno dell'unità congiunta per il ciberspazio e istituire una **piattaforma fisica** che consenta ai gruppi di svolgere attività tecniche e operative. Sulla base dei lavori preparatori svolti nella fase due, i partecipanti dovrebbero mettere a punto il piano dell'UE di risposta agli incidenti e alle crisi di cibersicurezza. I partecipanti operativi dovrebbero assicurarsi che gli esperti e le capacità inclusi nell'elenco delle capacità operative disponibili dell'UE siano effettivamente a disposizione e pronti a contribuire all'attività dei gruppi di reazione rapida dell'UE per la cibersicurezza.

Al fine di attuare il piano di risposta agli incidenti e alle crisi di cibersicurezza dell'UE, i partecipanti dovrebbero definire un programma di lavoro annuale.

AZIONI DI SOSTEGNO

La comunità della diplomazia informatica può avvalersi dell'unità congiunta per il ciberspazio per allineare la comunicazione pubblica. La piattaforma può consentire ai partecipanti di contribuire all'attribuzione politica, oltre che all'attribuzione nel contesto della giustizia penale a livello di polizia e giudiziario. Inoltre, può facilitare la ripresa e stimolare sinergie strutturate con le capacità di monitoraggio e rilevamento nazionali e transfrontaliere.

Per garantire l'operatività dell'unità congiunta per il ciberspazio, le azioni principali e, nella misura del possibile, quelle di sostegno della fase tre dovrebbero essere completate entro il **31 dicembre 2022 [6 mesi dopo la fine della fase 2]**.

4. *Fase 4 — Estendere la cooperazione nell'ambito dell'unità congiunta per il ciberspazio a soggetti privati e riferire sui progressi compiuti*

AZIONE PRINCIPALE

I partecipanti all'unità congiunta per il ciberspazio dovrebbero elaborare una **relazione di attività sui progressi compiuti nell'attuazione delle quattro fasi indicate nella raccomandazione, che descriva i risultati conseguiti e le sfide affrontate**. Tale relazione dovrebbe includere informazioni statistiche relative alle attività di cooperazione operativa svolte nel corso delle quattro fasi. La relazione dovrebbe essere presentata alla Commissione e all'alto rappresentante.

AZIONI DI SOSTEGNO

Al fine di estendere le capacità e le informazioni a disposizione dei gruppi di reazione rapida dell'UE per la cibersicurezza, i partecipanti dovrebbero garantire che l'unità congiunta per il ciberspazio fornisca assistenza alla conclusione di **accordi per la condivisione delle informazioni e di cooperazione operativa tra i partecipanti e soggetti del settore privato** che forniscono, tra l'altro, servizi di intelligence sulle minacce e di risposta agli incidenti. Dovrebbero inoltre garantire, tra l'altro, che l'unità congiunta per il ciberspazio fornisca sostegno, mediante attività regolari di dialogo e condivisione di informazioni sulle minacce e sulle vulnerabilità, agli utenti di soluzioni di cibersicurezza, principalmente quelli che rientrano nell'ambito di applicazione della direttiva NIS o che sono riuniti nei **centri di condivisione e analisi delle informazioni (ISAC) a livello dell'UE**.

Gli Stati membri dovrebbero aiutare i soggetti che operano nel loro territorio, in particolare quelli che rientrano nell'ambito di applicazione della direttiva NIS, ad avere accesso e a contribuire ai dialoghi pubblico-privato con gli ISAC a livello dell'UE.

Per garantire un adeguato coinvolgimento del settore privato, le azioni principali e, nella misura del possibile, quelle di sostegno della fase quattro dovrebbero essere completate entro il **30 giugno 2023 [6 mesi dopo la fine della fase 3]**.

MODALITÀ DI MOBILITAZIONE RAPIDA DELLE CAPACITÀ OPERATIVE DELL'UE

SOGGETTI CHE FORNISCONO LE CAPACITÀ: i partecipanti operativi

SOGGETTI CHE GESTISCONO LE CAPACITÀ: i partecipanti, all'interno dell'unità congiunta per il ciberspazio, secondo i ruoli e le responsabilità concordati

Fase	Obiettivo	Compito	Azione principale	Azione di sostegno
Fase 1 — Definire Entro il **31 dicembre 2021 [6 mesi dopo l'adozione]**	PREPARAZIONE	**Individuazione delle capacità**	**I partecipanti operativi stilano un elenco delle capacità operative disponibili dell'UE.**	
Fase 2 — Prepararsi entro il **30 giugno 2022 [6 mesi dopo la fine della fase 1]**	PREPARAZIONE	**Definire le procedure e gli accordi pertinenti per attivare le capacità in caso di necessità**	**I partecipanti operativi predispongono il piano dell'UE di risposta agli incidenti e alle crisi di cibersicurezza (quadro dell'UE di risposta alle crisi di cibersicurezza nell'ambito del programma), sulla base dei piani nazionali adottati**	**I partecipanti operativi elaborano relazioni integrate unionali sulla situazione basate sulla relazione sulla situazione tecnica della cibersicurezza nell'Unione**
	PREPARAZIONE	**Esercitazioni delle capacità**	Piano dell'UE di risposta agli incidenti e alle crisi di cibersicurezza	**I partecipanti organizzano esercitazioni e formazioni congiunte (tra comunità)** **I partecipanti elaborano un piano pluriennale per coordinare le esercitazioni.**
	CONSAPEVOLEZZA SITUAZIONALE	**Predisporre strumenti per condividere informazioni e richieste di sostegno**		**I partecipanti sviluppano modalità di condivisione sicura e rapida delle informazioni**
L'UNITÀ CONGIUNTA PER IL CIBERSPAZIO È OPERATIVA Sulla base del lavoro preparatorio svolto dai partecipanti in un gruppo di lavoro che sarà istituito dalla Commissione				
Fase 3 — Mobilitare entro il **31 dicembre 2022 [6 mesi dopo la fine della fase 2]**	PREPARAZIONE	**Adottare le procedure, gli accordi e i memorandum d'intesa pertinenti per attivare le capacità in caso di necessità**	**I partecipanti operativi mettono a punto il piano dell'UE di risposta agli incidenti e alle crisi di cibersicurezza e ne definiscono l'attuazione mediante programmi di lavoro annuali.**	**I partecipanti sostengono la creazione di capacità nazionali e transfrontaliere di monitoraggio e rilevamento, compresa la creazione dei SOC**
	RISPOSTA COORDINATA	**Mobilitare le capacità in caso di necessità**	**I partecipanti operativi coordinano i gruppi operativi di reazione rapida dell'UE per la cibersicurezza attraverso la piattaforma virtuale e fisica dell'unità congiunta per il ciberspazio a Bruxelles.**	**I partecipanti coordinano la comunicazione pubblica e contribuiscono all'attribuzione politica, oltre che all'attribuzione nel contesto della giustizia penale**

Fase 4 — Espandere e riferire entro il **30 giugno 2023 [6 mesi dopo la fine della fase 3]**	CONSAPEVOLEZZA SITUAZIONALE RISPOSTA COORDINATA	**Garantire la scalabilità coinvolgendo il settore privato per far fronte alle esigenze emergenti**	**I partecipanti presentano una relazione di attività sui progressi compiuti, descrivendo i risultati conseguiti e le sfide affrontate con il sostegno di informazioni statistiche.**	**I partecipanti concludono accordi di condivisione delle informazioni e di cooperazione operativa con i fornitori di cibersicurezza** **I partecipanti concludono accordi di condivisione delle informazioni con gli utenti della cibersicurezza, principalmente i soggetti che rientrano nell'ambito di applicazione della direttiva NIS e gli UE-ISAC**