RACCOMANDAZIONI

RACCOMANDAZIONE (UE) 2017/1584 DELLA COMMISSIONE

del 13 settembre 2017

relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala

LA COMMISSIONE EUROPEA,

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

considerando quanto segue:

(1) L'utilizzo delle tecnologie dell'informazione e della comunicazione e la dipendenza dalle stesse sono diventati fondamentali in tutti i settori di attività economica, dato che imprese e cittadini dell'Unione sono più che mai interconnessi e interdipendenti a livello transettoriale e transfrontaliero. Un incidente di cibersicurezza che interessa le organizzazioni di più Stati membri o addirittura l'intera Unione, con potenziali gravi perturbazioni del mercato interno e più in generale delle reti e dei sistemi informativi dai quali dipendono l'economia, la democrazia e la società dell'Unione, è uno scenario per il quale gli Stati membri e le istituzioni dell'UE devono essere ben preparati.

(2) Un incidente di cibersicurezza può essere considerato una crisi a livello di Unione quando le conseguenti perturbazioni sono talmente ampie da non poter essere gestite autonomamente dallo Stato membro interessato o quando interessa due o più Stati membri e ha un impatto di rilevanza tecnica o politica di così vasta portata da richiedere un coordinamento e una risposta tempestivi a livello politico dell'Unione.

(3) Gli incidenti di cibersicurezza possono innescare crisi più ampie, con ripercussioni su altri settori di attività al di là delle reti e dei sistemi informativi e delle reti di comunicazione; per reagire adeguatamente è necessario intervenire con attività di attenuazione concernenti sia l'ambito informatico che altri ambiti.

(4) Gli incidenti di cibersicurezza sono imprevedibili e spesso si verificano ed evolvono in tempi molto ridotti, pertanto i soggetti colpiti e coloro che hanno la responsabilità di reagire e di attenuare gli effetti conseguenti devono coordinare la loro risposta rapidamente. Inoltre, spesso tali incidenti non sono circoscritti a una determinata area geografica e possono verificarsi simultaneamente o diffondersi all'istante in molti paesi.

(5) Una risposta efficace agli incidenti e alle crisi di cibersicurezza su vasta scala a livello dell'UE richiede una cooperazione rapida ed efficace tra tutti i portatori di interesse e dipende dalla preparazione e dalle capacità dei singoli Stati membri, come pure da un'azione comune coordinata sostenuta dalle capacità dell'Unione. Per rispondere in modo tempestivo ed efficace agli incidenti sono pertanto necessari procedure e meccanismi di cooperazione stabiliti in precedenza e, per quanto possibile, ben collaudati che definiscano con chiarezza i ruoli e le responsabilità dei principali attori a livello nazionale e di Unione.

(6) Nelle sue conclusioni ([1]) sulla protezione delle infrastrutture critiche informatizzate del 27 maggio 2011 il Consiglio ha invitato gli Stati membri dell'UE a «rafforzare la collaborazione tra gli Stati membri e contribuire, sulla base di esperienze e risultati nazionali in materia di gestione delle crisi e in collaborazione con l'ENISA, a sviluppare i meccanismi di una cooperazione europea in materia di incidenti informatici, da saggiare nel contesto della prossima esercitazione "Europa informatica" nel 2012».

(7) Nella sua comunicazione del 2016 dal titolo «Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza» ([2]) la Commissione ha incoraggiato gli Stati membri a sfruttare al massimo i meccanismi di cooperazione della direttiva sulla sicurezza delle reti e dell'informazione (direttiva NIS) ([3]), come pure a rafforzare la cooperazione transfrontaliera per poter fronteggiare

([1]) Conclusioni del Consiglio sulla comunicazione dal titolo «Protezione delle infrastrutture critiche informatizzate — Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale», documento 10299/11, Bruxelles, 27 maggio 2011.
([2]) COM(2016) 410 final del 5 luglio 2016.
([3]) 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).

un incidente cibernetico su vasta scala. Ha inoltre aggiunto che la capacità di fronteggiare gli incidenti informatici su vasta scala trarrebbe vantaggio da un approccio coordinato alla cooperazione tra i vari elementi dell'ecosistema cibernetico nelle situazioni di crisi; tale approccio dovrebbe essere definito in un «programma» e dovrebbe anche garantire sinergie e coerenza con i meccanismi esistenti di gestione delle crisi.

(8) Nelle conclusioni del Consiglio ([1]) sulla comunicazione di cui sopra gli Stati membri hanno invitato la Commissione a presentare un tale programma da sottoporre alla valutazione degli organismi e delle altre parti interessate. La direttiva NIS tuttavia non prevede un quadro di cooperazione dell'Unione in caso di incidenti e crisi di cibersicurezza su vasta scala.

(9) La Commissione ha consultato gli Stati membri in due distinti seminari di consultazione, svoltisi a Bruxelles il 5 aprile e il 4 luglio 2017, ai quali hanno partecipato rappresentanti degli Stati membri dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), del gruppo di cooperazione istituito dalla direttiva NIS e del gruppo orizzontale del Consiglio per le questioni riguardanti il ciberspazio, nonché rappresentanti del Servizio europeo per l'azione esterna (SEAE), dell'ENISA, di Europol/EC3 e del segretariato generale del Consiglio (SGC).

(10) Il programma per una risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala a livello dell'Unione, riportato nell'allegato della presente raccomandazione, è il risultato delle consultazioni di cui sopra e integra la comunicazione «Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza».

(11) Il programma descrive e definisce gli obiettivi e le modalità della cooperazione tra gli Stati membri e le istituzioni, gli organi, gli uffici e le agenzie dell'UE (di seguito «istituzioni dell'UE») in risposta agli incidenti e alle crisi di cibersicurezza su vasta scala, indicando altresì in che modo i meccanismi esistenti di gestione delle crisi possono fare pieno ricorso ai soggetti esistenti a livello dell'UE incaricati della cibersicurezza.

(12) Nel rispondere a una crisi di cibersicurezza ai sensi del considerando 2, il coordinamento della risposta a livello politico dell'Unione in seno al Consiglio si avvarrà dei dispositivi integrati per la risposta politica alle crisi (IPCR) ([2]); la Commissione farà ricorso al processo di coordinamento delle crisi transettoriale ad alto livello del sistema ARGUS ([3]). Per le crisi che presentano un'importante dimensione esterna o una forte correlazione con la politica di sicurezza e di difesa comune (PSDC) sarà attivato il meccanismo di risposta alle crisi ([3]) del Servizio europeo per l'azione esterna (SEAE).

(13) In alcuni settori i meccanismi di gestione delle crisi settoriali a livello di UE prevedono la cooperazione in caso di incidenti o crisi di cibersicurezza. Ad esempio, nel quadro del sistema globale di navigazione satellitare (GNSS), la decisione 2014/496/PESC del Consiglio ([4]), già definisce i rispettivi ruoli del Consiglio, dell'Alto rappresentante, della Commissione, dell'Agenzia del GNSS europeo e degli Stati membri nell'ambito della catena di responsabilità operative definite per reagire a una minaccia per l'Unione, gli Stati membri o il GNSS, anche in caso di attacchi cibernetici. La presente raccomandazione pertanto non dovrebbe lasciare impregiudicati tali meccanismi.

(14) Gli Stati membri hanno la responsabilità primaria di reagire in caso di incidenti o crisi di cibersicurezza su vasta scala che li riguardino. La Commissione, l'Alto rappresentante e le altre istituzioni o gli altri servizi dell'UE hanno tuttavia un ruolo importante, derivante dal diritto dell'Unione o dal fatto che gli incidenti e le crisi di cibersicurezza possono avere ripercussioni su tutti i settori dell'attività economica nell'ambito del mercato unico, sulla sicurezza e sulle relazioni internazionali dell'Unione e sulle istituzioni stesse.

(15) A livello di Unione, i principali soggetti coinvolti nella risposta alle crisi di cibersicurezza comprendono le strutture e i meccanismi previsti dalla direttiva NIS recentemente istituiti, vale a dire la rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), come pure le agenzie e gli organismi competenti, ossia l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), il Centro europeo per la lotta alla criminalità informatica di Europol (Europol/EC3), il Centro dell'UE di analisi dell'intelligence (INTCEN), la direzione di intelligence dello Stato maggiore dell'Unione europea (EUMS INT) e la sala situazione (SITROOM) che collaborano come capacità unica di analisi dell'intelligence (SIAC), la cellula dell'UE per l'analisi delle minacce ibride (presso l'INTCEN), la squadra di pronto intervento informatico delle istituzioni dell'UE (CERT-UE) e il Centro di coordinamento della risposta alle emergenze della Commissione europea.

(16) La cooperazione tra gli Stati membri per reagire agli incidenti di cibersicurezza a livello tecnico è assicurata dalla rete dei CSIRT istituita dalla direttiva NIS. L'ENISA svolge la funzione di segretariato della rete e sostiene

([1]) Documento 14540/16, 15 novembre 2016.
([2]) Ulteriori informazioni sono disponibili nella sezione 3.1. dell'appendice sulla gestione delle crisi, sui meccanismi di cooperazione e sugli attori a livello di UE.
([3]) Ibidem.
([4]) Decisione 2014/496/PESC del Consiglio, del 22 luglio 2014, sugli aspetti del dispiegamento, del funzionamento e dell'utilizzo del sistema globale di navigazione via satellite europeo che hanno incidenza sulla sicurezza dell'Unione europea e che abroga l'azione comune 2004/552/PESC (GU L 219 del 25.7.2014, pag. 53).

attivamente la cooperazione fra i CSIRT. I CSIRT nazionali e il CERT-UE collaborano e si scambiano informazioni su base volontaria, se necessario anche in risposta a incidenti di cibersicurezza che interessano uno o più Stati membri. Su richiesta di un rappresentante del CSIRT di uno Stato membro, possono discutere e, ove possibile, individuare un intervento coordinato per un incidente rilevato nella giurisdizione dello Stato membro in questione. Le procedure pertinenti saranno definite nell'ambito delle procedure operative standard (POS) della rete dei CSIRT ([1]).

(17) La rete dei CSIRT ha inoltre il compito di discutere, esaminare e individuare ulteriori forme di cooperazione operativa, anche in relazione alle categorie di rischi e di incidenti, all'allerta precoce, all'assistenza reciproca, ai principi e alle modalità di coordinamento, quando gli Stati membri intervengono a proposito di rischi e incidenti transfrontalieri.

(18) Il gruppo di cooperazione istituito dall'articolo 11 della direttiva NIS ha il compito di fornire orientamenti strategici per le attività della rete dei CSIRT, di discutere della capacità e dello stato di preparazione degli Stati membri e, su base volontaria, di valutare le strategie nazionali in materia di sicurezza della rete e dei sistemi informativi e l'efficacia dei CSIRT e di individuare le migliori pratiche.

(19) Un *workstream* dedicato all'interno del gruppo di cooperazione sta elaborando orientamenti in materia di notifica degli incidenti, a norma dell'articolo 14, paragrafo 7, della direttiva NIS, concernenti i casi in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti a norma dell'articolo 14, paragrafo 3, e il formato e la procedura di tali notifiche ([2]).

(20) La conoscenza e la comprensione della situazione in tempo reale, della posizione di rischio e delle minacce, acquisite attraverso relazioni, valutazioni, ricerche, indagini e analisi, sono fondamentali per poter prendere decisioni con cognizione di causa. La «conoscenza situazionale» da parte di tutte le parti interessate è essenziale per l'efficacia della risposta coordinata. La conoscenza situazionale comprende gli elementi relativi alle cause, all'impatto e all'origine dell'incidente. È risaputo che essa dipende dallo scambio e dalla condivisione di informazioni tra le parti interessate in un formato idoneo, mediante il ricorso a una tassonomia comune per la descrizione dell'incidente e secondo modalità sicure.

(21) La risposta agli incidenti di cibersicurezza può assumere molte forme, che vanno dall'individuazione di misure tecniche che possono comportare la ricerca congiunta — da parte di due o più soggetti — delle cause tecniche dell'incidente (ad esempio, analisi dei programmi malevoli, noti anche come *malware*) o l'identificazione dei modi in cui le organizzazioni possono valutare se sono state colpite (ad esempio, indicatori di compromissione) alle decisioni operative sull'applicazione di tali misure e, a livello politico, sulla scelta di ricorrere ad altri strumenti, ad esempio al quadro relativo a una risposta comune alle attività informatiche dolose ([3]) o al protocollo operativo dell'UE per contrastare le minacce ibride ([4]), in funzione dell'incidente.

(22) La fiducia dei cittadini e delle imprese europei nei servizi digitali è essenziale per un mercato unico digitale fiorente. Pertanto, la comunicazione in caso di crisi riveste un ruolo particolarmente importante nell'attenuazione degli effetti negativi degli incidenti e delle crisi di cibersicurezza. La comunicazione può essere utilizzata anche nell'ambito del quadro relativo a una risposta diplomatica comune come strumento per influenzare il comportamento dei (potenziali) aggressori che agiscono da paesi terzi. L'allineamento della comunicazione pubblica per attenuare gli effetti negativi degli incidenti e delle crisi di cibersicurezza e l'uso della comunicazione pubblica per influenzare un aggressore sono essenziali per dare efficacia alla risposta politica.

(23) Informare la popolazione su come attenuare, a livello di utente e di organizzazione, gli effetti di un incidente (ad esempio mediante l'applicazione di aggiornamenti di sicurezza o il ricorso ad azioni complementari per evitare la minaccia) potrebbe essere una misura efficace per ridurre l'impatto di un incidente o di una crisi di cibersicurezza su vasta scala.

(24) La Commissione, attraverso l'infrastruttura di servizi digitali per la cibersicurezza del Meccanismo per collegare l'Europa (MCE), sta sviluppando un meccanismo di cooperazione basato su una piattaforma di servizi essenziali (noto come MeliCERTes) tra i CSIRT degli Stati membri partecipanti per migliorare il loro livello di preparazione, cooperazione e reazione alle minacce e agli incidenti cibernetici emergenti. La Commissione, mediante inviti a presentare proposte su base concorrenziale per la concessione di sovvenzioni nell'ambito dell'MCE cofinanzia i CSIRT negli Stati membri al fine di migliorare le loro capacità operative a livello nazionale.

([1]) In corso di elaborazione; dovrebbero essere adottate entro la fine del 2017.
([2]) Gli orientamenti dovrebbero essere completati entro la fine del 2017.
([3]) Conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose («pacchetto di strumenti della diplomazia informatica»), documento 9916/17.
([4]) Documento di lavoro dei servizi della Commissione: «EU operational protocol for countering hybrid threats "EU Playbook"», SWD(2016) 227 final del 5 luglio 2016.

(25) Per promuovere e migliorare la collaborazione tra Stati membri e settore privato è fondamentale organizzare esercitazioni sugli incidenti cibernetici a livello dell'UE. A tal fine, dal 2010 l'ENISA organizza regolarmente esercitazioni paneuropee sugli incidenti cibernetici («Cyber Europe»).

(26) Nelle sue conclusioni ([1]) sull'attuazione della dichiarazione congiunta del presidente del Consiglio europeo, del presidente della Commissione europea e del segretario generale dell'Organizzazione del trattato del Nord Atlantico, il Consiglio chiede il rafforzamento della cooperazione nelle esercitazioni di cibersicurezza attraverso la reciproca partecipazione del personale alle rispettive esercitazioni, comprese in particolare Cyber Coalition e Cyber Europe.

(27) Il panorama delle minacce in costante evoluzione e i recenti incidenti di cibersicurezza sono un'indicazione del rischio crescente cui deve far fronte l'Unione; gli Stati membri dovrebbero dar seguito alla presente raccomandazione senza ulteriore indugio e in ogni caso entro la fine del 2018,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

(1) Gli Stati membri e le istituzioni dell'UE dovrebbero istituire un quadro di risposta alle crisi di cibersicurezza dell'UE che integri gli obiettivi e le modalità di cooperazione descritti nel programma attenendosi ai principi guida ivi riportati.

(2) Il quadro di risposta alle crisi di cibersicurezza dell'UE dovrebbe in particolare individuare i soggetti interessati, le istituzioni dell'UE e le autorità degli Stati membri competenti a tutti i livelli necessari — tecnico, operativo, strategico/politico — ed elaborare, ove necessario, procedure operative standard che definiscano le modalità di cooperazione dei soggetti di cui sopra nell'ambito dei meccanismi UE di gestione delle crisi. L'accento dovrebbe essere posto sulla necessità di consentire lo scambio di informazioni senza indebiti ritardi e sul coordinamento della risposta durante gli incidenti e le crisi di cibersicurezza su vasta scala.

(3) A tal fine, le autorità competenti degli Stati membri dovrebbero collaborare per specificare ulteriormente i protocolli per la condivisione delle informazioni e la cooperazione. Il gruppo di cooperazione dovrebbe procedere allo scambio delle esperienze acquisite in materia con le competenti istituzioni dell'UE.

(4) Gli Stati membri dovrebbero provvedere affinché i meccanismi nazionali di gestione delle crisi reagiscano in modo adeguato agli incidenti di cibersicurezza e creare le procedure necessarie per la cooperazione a livello dell'UE nell'ambito del quadro dell'UE.

(5) In linea con il programma, gli Stati membri dovrebbero, in collaborazione con i servizi della Commissione e il SEAE, stabilire orientamenti per l'attuazione pratica per quanto riguarda l'integrazione delle loro procedure e dei soggetti nazionali incaricati della gestione delle crisi e della cibersicurezza nei vigenti meccanismi dell'UE di gestione delle crisi, vale a dire l'IPCR e il CRM del SEAE. In particolare, gli Stati membri dovrebbero garantire che vengano predisposte le strutture appropriate per consentire un flusso di informazioni efficiente tra le rispettive autorità nazionali di gestione delle crisi e i loro rappresentanti a livello dell'UE nell'ambito dei meccanismi UE di gestione delle crisi.

(6) Gli Stati membri dovrebbero avvalersi pienamente delle opportunità offerte dal programma delle infrastrutture di servizi digitali del Meccanismo per collegare l'Europa (MCE) e collaborare con la Commissione per garantire che il meccanismo di cooperazione della piattaforma di servizi essenziali, attualmente in corso di sviluppo, fornisca le funzionalità necessarie e soddisfi i requisiti per la cooperazione anche durante le crisi di cibersicurezza.

(7) Gli Stati membri, con l'assistenza dell'ENISA e sulla base del lavoro già svolto in questo ambito, dovrebbero cooperare all'elaborazione e all'adozione di una tassonomia e di un modello comuni per la descrizione delle cause tecniche e delle ripercussioni degli incidenti di cibersicurezza nelle relazioni sulla situazione, al fine di rafforzare ulteriormente la cooperazione tecnica e operativa durante le crisi. A tale riguardo, gli Stati membri dovrebbero tener conto dei lavori in corso nell'ambito del gruppo di cooperazione sugli orientamenti in materia di notifica degli incidenti, in particolare, degli aspetti relativi al formato delle notifiche nazionali.

(8) Le procedure stabilite nel quadro dovrebbero essere provate e, se necessario, rivedute a seguito degli insegnamenti tratti dalla partecipazione degli Stati membri alle esercitazioni di cibersicurezza a livello nazionale, regionali, dell'Unione e della NATO, nonché nell'ambito della diplomazia cibernetica. Dovrebbero essere provate in particolare nel quadro delle esercitazioni Cyber Europe organizzate dall'ENISA. Cyber Europe 2018 offre per la prima volta questa opportunità.

([1]) ST 15283/16, 6 dicembre 2016.

(9) Gli Stati membri e le istituzioni dell'UE dovrebbero organizzare regolarmente esercitazioni per verificare la loro risposta agli incidenti e alle crisi di cibersicurezza su vasta scala a livello nazionale ed europeo, anche per quanto riguarda la risposta politica, se del caso coinvolgendo soggetti del settore privato.

Fatto a Bruxelles, il 13 settembre 2017

Per la Commissione

Mariya GABRIEL

Membro della Commissione

ALLEGATO

Programma per una risposta coordinata agli incidenti e alle crisi di cibersicurezza transfrontalieri su vasta scala

INTRODUZIONE

Il presente programma si applica agli incidenti di cibersicurezza che causano perturbazioni talmente ampie da non poter essere gestite autonomamente dallo Stato membro interessato o che interessano due o più Stati membri o istituzioni dell'UE e hanno un impatto di rilevanza tecnica o politica di così vasta portata da richiedere un coordinamento politico e una risposta tempestivi a livello di Unione.

Gli incidenti di cibersicurezza su vasta scala sono da considerarsi al pari di una «crisi» di cibersicurezza.

In caso di crisi a livello di UE che presenti elementi di cibersicurezza, il coordinamento della risposta a livello politico dell'Unione deve essere effettuato dal Consiglio mediante i dispositivi integrati per la risposta politica alle crisi (IPCR).

All'interno della Commissione il coordinamento avviene conformemente al sistema di allarme rapido ARGUS.

Per le crisi che presentano un'importante dimensione esterna o una forte correlazione con la politica di sicurezza e di difesa comune (PSDC) viene attivato il meccanismo di risposta alle crisi del SEAE.

Il programma descrive il modo in cui tali meccanismi ben consolidati per la gestione delle crisi devono fare pieno ricorso ai soggetti esistenti a livello dell'UE incaricati della cibersicurezza, nonché ai meccanismi di cooperazione tra gli Stati membri.

A tal fine, il programma tiene conto di una serie di principi guida (proporzionalità, sussidiarietà, complementarità e riservatezza delle informazioni) e indica gli obiettivi principali della cooperazione (risposta efficace, conoscenza situazionale condivisa, messaggi di comunicazione pubblica) a tre livelli (strategico/politico, operativo e tecnico), i meccanismi, i soggetti coinvolti e le attività da svolgere per conseguire gli obiettivi principali di cui sopra.

Il programma non copre l'intero ciclo di gestione delle crisi (prevenzione/attenuazione, preparazione, risposta, ripristino) ma si concentra sulla risposta. Ciononostante contempla alcune attività, in particolare quelle correlate al conseguimento di una conoscenza situazionale condivisa.

È altresì importante osservare che gli incidenti di cibersicurezza possono scatenare una crisi più ampia, o essere parte di una tale crisi, e avere quindi ripercussioni in altri ambiti. Dato che si presume che la maggior parte delle crisi di cibersicurezza abbiano un impatto sul mondo fisico, qualsiasi risposta adeguata deve basarsi su attività di attenuazione concernenti sia l'ambito informatico che altri ambiti. L'attività di risposta alle crisi cibernetiche dovrebbero essere coordinate con altri meccanismi di gestione delle crisi a livello UE, nazionale o settoriale.

Infine, il programma non sostituisce, e lascia pertanto impregiudicati, i meccanismi, le disposizioni o gli strumenti specifici per determinati settori o politiche, come lo strumento istituito per il programma del sistema globale europeo di navigazione satellitare (GNSS) [1].

Principi guida

Nello svolgimento delle attività finalizzate al conseguimento degli obiettivi, nell'individuazione delle attività necessarie e nell'attribuzione dei ruoli e delle responsabilità ai soggetti o ai meccanismi, sono stati applicati i seguenti principi guida, che devono essere rispettati anche nell'elaborazione delle future linee guida di attuazione.

Proporzionalità: la stragrande maggioranza degli incidenti di cibersicurezza che colpiscono gli Stati membri hanno una portata di gran lunga inferiore a quella che permetterebbe di considerarli alla stregua di una «crisi» nazionale, tanto meno una crisi europea. La base della cooperazione tra gli Stati membri nel reagire a tali incidenti è fornita dalla rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) istituita dalla direttiva NIS [2]. I CSIRT nazionali collaborano e si scambiano informazioni su base volontaria e giornaliera, se necessario anche in risposta a incidenti di cibersicurezza che interessano uno o più Stati membri, in linea con le procedure operative standard (POS) della rete dei CSIRT. Il programma dovrebbe pertanto prevedere il pieno ricorso alle POS, che dovrebbero contemplare ulteriori compiti specifici per le crisi di cibersicurezza.

[1] Decisione 2014/496/PESC.
[2] Direttiva (UE) 2016/1148.

Sussidiarietà: il principio di sussidiarietà è fondamentale. Gli Stati membri hanno la responsabilità primaria di reagire in caso di incidenti o crisi di cibersicurezza su vasta scala che li riguardino. La Commissione, il Servizio europeo per l'azione esterna e le istituzioni, gli organi, gli uffici e le agenzie dell'UE hanno tuttavia un ruolo importante. Tale ruolo è definito chiaramente nei dispositivi IPCR, ma deriva anche dal diritto dell'Unione o semplicemente dal fatto che gli incidenti e le crisi di cibersicurezza possono avere ripercussioni su tutti i settori dell'attività economica nel mercato unico, sulla sicurezza e sulle relazioni internazionali dell'Unione, nonché sulle istituzioni stesse.

Complementarità: il programma prende pienamente in considerazione i meccanismi di gestione delle crisi esistenti a livello UE, vale a dire i dispositivi integrati per la risposta politica alle crisi (IPCR), ARGUS e il meccanismo di risposta alle crisi del SEAE, vi integra le nuove strutture e i nuovi meccanismi previsti dalla direttiva NIS, ossia la rete dei CSIRT, come pure le agenzie e gli organismi competenti, ossia l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), il Centro europeo per la lotta alla criminalità informatica di Europol (Europol/EC3), il Centro dell'UE di analisi dell'intelligence (INTCEN), la direzione di intelligence dello Stato maggiore dell'Unione europea (EUMS INT) e la sala situazione (SITROOM) presso l'INTCEN, che collaborano come capacità unica di analisi dell'intelligence (SIAC); la cellula dell'UE per l'analisi delle minacce ibride (presso l'INTCEN); e la squadra di pronto intervento informatico per le istituzioni, gli organi e le agenzie dell'UE (CERT-UE). A tal fine, il programma dovrebbe anche garantire che la loro interazione e cooperazione avvengano all'insegna della massima complementarità e della minima sovrapposizione.

Riservatezza delle informazioni: Tutti gli scambi di informazioni nel contesto del programma devono essere conformi alle norme applicabili in materia di sicurezza ([1]) e di protezione dei dati personali e al protocollo TLP (Traffic Light Protocol) ([2]). Per lo scambio di informazioni classificate, indipendentemente dal sistema di classificazione utilizzato, dovrebbero essere utilizzati strumenti accreditati ([3]). Il trattamento dei dati personali avverrà nel rispetto delle norme UE applicabili, in particolare il regolamento generale sulla protezione dei dati ([4]), la direttiva relativa alla vita privata e alle comunicazioni elettroniche ([5]) e il regolamento ([6]) concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, nonché la libera circolazione di tali dati.

Obiettivi principali

La cooperazione nell'ambito del programma segue l'approccio a tre livelli di cui sopra: politico, operativo e tecnico. A ciascun livello la cooperazione, che può comprendere sia scambio di informazioni che azioni comuni, mira a conseguire gli obiettivi principali che si indicano di seguito.

— *Consentire una risposta efficace*. La risposta può assumere molte forme, che vanno dall'individuazione di misure tecniche che possono comportare la ricerca congiunta — da parte di due o più soggetti — delle cause tecniche dell'incidente (ad esempio analisi dei programmi malevoli (*malware*)] o l'identificazione dei modi in cui le organizzazioni possono valutare se sono state colpite (ad esempio indicatori di compromissione) alle decisioni operative sull'applicazione di tali misure tecniche e, a livello politico, sulla scelta di ricorrere ad altri strumenti quali la risposta diplomatica dell'UE alle attività informatiche dolose («pacchetto di strumenti della diplomazia informatica») o il protocollo operativo dell'UE per contrastare le minacce ibride, in funzione dell'incidente.

— *Condividere la conoscenza situazionale*. Per una risposta coordinata è fondamentale una buona comprensione degli eventi a mano a mano che si verificano da parte di tutti i portatori di interessi a tutti e tre i livelli (tecnico, operativo, politico). La conoscenza situazionale può comprendere gli elementi tecnologici relativi alle cause, all'impatto e all'origine dell'incidente. Dato che gli incidenti di cibersicurezza possono interessare numerosi settori (finanza, energia, trasporti, assistenza sanitaria ecc.), è indispensabile che le informazioni appropriate giungano a tutti i portatori di interessi in modo tempestivo e nel formato adeguato.

([1]) Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41) e decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate (GU L 72 del 17.3.2015, pag. 53); decisione dell'alto rappresentante dell'Unione per gli Affari esteri e la politica di sicurezza, del 19 aprile 2013, relativa alle norme di sicurezza del Servizio europeo per l'azione esterna (GU C 190 del 29.6.2013, pag. 1); decisione 2013/488/UE del Consiglio, del 23 settembre 2013, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 274 del 15.10.2013, pag. 1).

([2]) https://www.first.org/tlp/

([3]) A giugno 2016 questi canali di trasmissione comprendevano CIMS (sistema di gestione delle informazioni classificate), ACID (algoritmo di crittografia), RUE (sistema protetto per la creazione, lo scambio e l'archiviazione di documenti RESTREINT UE/EU RESTRICTED) e SOLAN. Tra gli altri mezzi, ad esempio per la trasmissione delle informazioni classificate, figurano PGP e S/MIME.

([4]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati (GU L 119 del 4.5.2016, pag. 1)).

([5]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

([6]) Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

— *Concordare i principali messaggi di comunicazione pubblica* ([1]). Le comunicazioni in caso di crisi svolgono un ruolo importante nel limitare gli effetti negativi degli incidenti e delle crisi di cibersicurezza, ma possono anche essere utilizzate come strumento per influenzare il comportamento dei (potenziali) aggressori. Un messaggio appropriato che segnala chiaramente le possibili conseguenze di una risposta diplomatica può anche servire a influenzare il comportamento degli aggressori. L'allineamento della comunicazione pubblica per attenuare gli effetti negativi degli incidenti e delle crisi di cibersicurezza e la comunicazione pubblica intesa a influenzare gli aggressori sono essenziali per dare efficacia alla risposta politica. Di particolare importanza nella cibersicurezza è la diffusione ai cittadini di informazioni accurate e utilizzabili su come attenuare le conseguenze di un incidente (ad esempio applicando aggiornamenti di sicurezza, effettuando azioni complementari per evitare la minaccia ecc.).

COOPERAZIONE A LIVELLO TECNICO, OPERATIVO E STRATEGICO/POLITICO TRA STATI MEMBRI E TRA STATI MEMBRI E SOGGETTI DELL'UE

Una risposta efficace agli incidenti o alle crisi di cibersicurezza su vasta scala a livello dell'UE dipende dall'efficacia della cooperazione tecnica, operativa e strategica/politica.

A ciascun livello i soggetti coinvolti dovrebbero svolgere attività specifiche per il raggiungimento di tre obiettivi principali:

— risposta coordinata,

— condivisione della conoscenza situazionale,

— comunicazioni pubbliche.

Per tutta la durata dell'incidente o della crisi, i livelli inferiori della cooperazione allertano, informano e sostengono i livelli superiori, mentre i livelli superiori forniscono orientamenti ([2]) e prendono decisioni per i livelli inferiori, a seconda dei casi.

Cooperazione a livello tecnico

Ambito delle attività:

— trattamento dell'incidente ([3]) durante una crisi di cibersicurezza,

— monitoraggio e sorveglianza dell'incidente, compresa l'analisi continua delle minacce e dei rischi.

Soggetti potenziali

A livello tecnico, il programma individua il meccanismo centrale di cooperazione nella rete dei CSIRT, presieduta dalla presidenza e il cui segretariato è fornito dall'ENISA.

— Stati membri:

  — autorità competenti e punti di contatto unici istituiti dalla direttiva NIS

  — CSIRT

— Organismi/uffici/agenzie dell'UE:

  — ENISA

  — Europol/EC3

  — CERT-UE

([1]) È importante notare che per comunicazione pubblica si può intendere sia la comunicazione dell'incidente al pubblico in generale sia la comunicazione di ulteriori informazioni tecniche od operative ai settori critici e/o a coloro che sono stati colpiti. Ciò può richiedere l'utilizzo di canali di diffusione riservati e l'uso di specifici strumenti tecnici/piattaforme. In entrambi i casi la comunicazione con gli operatori e il pubblico in generale all'interno degli Stati membri è di competenza e responsabilità di ciascuno Stato membro. Pertanto, in linea con il principio di sussidiarietà di cui sopra, gli Stati membri e i CSIRT nazionali hanno la responsabilità finale delle informazioni diffuse rispettivamente all'interno del loro territorio e presso le comunità di loro competenza.

([2]) «Autorizzazione ad agire»: in una crisi di cibersicurezza è di vitale importanza che i tempi di reazione siano rapidi, per definire le opportune azioni di attenuazione. Al fine di garantire questi tempi di reazione rapidi, uno Stato membro può emanare un'«autorizzazione ad agire» volontaria nei confronti di un altro Stato membro, dandogli il permesso di agire immediatamente, senza doversi consultare con i livelli superiori o con le istituzioni dell'UE e passare attraverso tutti i canali ufficiali normalmente richiesti, se ciò non richiesto in un determinato incidente (ad esempio, un CSIRT non dovrebbe consultarsi con i livelli superiori per trasmettere informazioni utili a un CSIRT in un altro Stato membro).

([3]) Per «trattamento dell'incidente» si intendono tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente.

— Commissione europea:

  — il Centro di coordinamento della risposta alle emergenze (ERCC) (servizio operativo attivo 24 ore su 24, 7 giorni su 7 presso la DG ECHO) e il servizio capofila designato (da scegliere tra la DG CNECT e la DG HOME in funzione della natura specifica dell'incidente), il segretariato generale (segretariato ARGUS), la DG HR (direzione Sicurezza), la DG DIGIT (Aspetti operativi della sicurezza informatica)

  — per le altre agenzie dell'UE ([1]) la rispettiva DG di riferimento della Commissione o del SEAE (primo punto di contatto)

— SEAE:

  — capacità unica di analisi dell'intelligence (SIAC: INTCEN dell'UE e EUMS INT)

  — sala situazione dell'UE e servizi geografici o tematici designati

  — cellula dell'UE per l'analisi delle minacce ibride (parte dell'INTCEN dell'UE: cibersicurezza in un contesto ibrido).

Condivisione della conoscenza situazionale

— Nell'ambito della costante cooperazione a livello tecnico per sostenere la conoscenza situazionale dell'Unione, l'ENISA dovrebbe elaborare periodicamente la relazione sulla situazione tecnica della cibersicurezza nell'UE in merito alle minacce e agli incidenti, sulla base delle informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise di CSIRT degli Stati membri (su base volontaria) o dai punti di contatto unici istituiti dalla direttiva NIS, dal Centro europeo per la lotta alla criminalità informatica (EC3) presso Europol, dal CERT-UE e, ove necessario, dal Centro dell'UE di analisi dell'intelligence (INTCEN) presso il Servizio europeo per l'azione esterna (SEAE). La relazione dovrebbe essere messa a disposizione delle istanze competenti del Consiglio, della Commissione, dell'AR/VP e della rete dei CSIRT.

— In caso di incidente grave il presidente della rete dei CSIRT, assistito dall'ENISA, elabora una relazione sulla situazione degli incidenti di cibersicurezza nell'UE ([2]), che viene presentata alla presidenza, alla Commissione e all'AR/VP attraverso il CSIRT della presidenza di turno.

— *Tutte le altre agenzie dell'UE* riferiscono alle loro rispettive DG di riferimento, che a loro volta riferiscono al servizio capofila della Commissione.

— *CERT-UE* fornisce relazioni tecniche alla rete dei CSIRT, alle istituzioni e alle agenzie dell'UE (se necessario) e ad ARGUS (se attivato).

— *Europol/EC3* ([3]) *e CERT-UE* forniscono l'analisi forense effettuata da esperti degli artefatti tecnici e altre informazioni tecniche alla rete dei CSIRT.

— SEAE SIAC: la cellula dell'UE per l'analisi delle minacce ibride riferisce, per conto dell'INTCEN, ai pertinenti dipartimenti del SEAE.

Risposta

— *La rete dei CSIRT* scambia informazioni e analisi tecniche sull'incidente, quali indirizzi IP, indicatori di compromissione ([4]) ecc. Tali informazioni devono essere fornite all'ENISA senza indebito ritardo ed entro 24 ore dal momento in cui l'incidente viene individuato.

— Secondo le procedure operative standard della rete dei CSIRT, i membri collaborano negli sforzi volti ad analizzare gli artefatti tecnici disponibili e altre informazioni tecniche relative all'incidente, al fine di stabilirne le cause e le possibili misure tecniche di attenuazione.

— L'ENISA assiste i CSIRT nelle loro attività tecniche, basandosi sulla propria competenza e conformemente al suo mandato ([5]).

([1]) In base alla natura e all'impatto dell'incidente nei diversi settori di attività (finanza, trasporti, energia, assistenza sanitaria ecc.) saranno coinvolte le agenzie o gli organi pertinenti dell'Unione.

([2]) La relazione sulla situazione degli incidenti di cibersicurezza nell'UE è elaborata aggregando le relazioni nazionali fornite dai CSIRT nazionali. Il formato della relazione dovrebbe essere descritto nelle procedure operative standard (POS) della rete dei CSIRT.

([3]) In conformità alle condizioni e alle procedure stabilite nel quadro giuridico dell'EC3.

([4]) Indicatore di compromissione (IOC): nell'informatica legale è un artefatto osservato in una rete o in un sistema operativo che indica con elevato livello di attendibilità l'intrusione in un computer. Tipici indicatori di compromissione sono le firme e gli indirizzi IP del virus, gli *hash* MD5 dei file di programmi malevoli o gli URL o i nomi di dominio dei server di comando e controllo delle *botnet*.

([5]) Proposta di regolamento relativo all'ENISA, l'agenzia dell'UE per la sicurezza informatica, che abroga il regolamento (UE) n. 526/2013, e alla certificazione di cibersicurezza per le tecnologie dell'informazione e della comunicazione («regolamento sulla cibersicurezza»), 13 settembre 2017.

— I CSIRT degli Stati membri coordinano le loro attività tecniche di risposta con l'assistenza dell'ENISA e della Commissione.

— SEAE SIAC: la cellula dell'UE per l'analisi delle minacce ibride lancia, per conto dell'INTCEN, la procedura per raccogliere gli elementi di prova iniziali.

Comunicazioni pubbliche

— I CSIRT elaborano consigli tecnici ([1]) e allarmi sulla vulnerabilità ([2]) e li diffondono alle rispettive comunità e al pubblico in base alle procedure di autorizzazione applicabili in ciascun caso.

— L'ENISA facilita la produzione e la diffusione delle comunicazioni comuni della rete dei CSIRT.

— L'ENISA coordina le proprie attività di comunicazione pubblica con la rete dei CSIRT e il servizio del portavoce della Commissione.

— L'ENISA e l'EC3 coordinano le loro attività di comunicazione pubblica in base alla conoscenza situazionale condivisa concordata tra gli Stati membri. Entrambi coordinano le loro attività di comunicazione pubblica con il servizio del portavoce della Commissione.

— Se la crisi comporta una dimensione esterna o di politica di sicurezza e di difesa comune (PSDC), la comunicazione pubblica dovrebbe essere coordinata con il SEAE e il servizio del portavoce dell'AR/VP.

Cooperazione a livello operativo

Ambito delle attività:

— preparare il processo decisionale a livello politico,

— coordinare la gestione delle crisi di cibersicurezza (se necessario)

— valutare le conseguenze e l'impatto a livello dell'UE e proporre eventuali misure di attenuazione

Soggetti potenziali

— Stati membri:

  — autorità competenti e punti di contatto unici istituiti dalla direttiva NIS

  — CSIRT, agenzie per la sicurezza informatica

  — altre autorità settoriali nazionali (in caso di incidenti o crisi multisettoriali).

— Organismi/uffici/agenzie dell'UE:

  — ENISA

  — Europol/EC3

  — CERT-UE

— Commissione europea:

  — il segretario generale (aggiunto) SG (procedura ARGUS),

  — DG CNECT/HOME

  — l'autorità di sicurezza della Commissione

  — altre DG (in caso di incidenti o crisi multisettoriali)

([1]) Consulenza di natura tecnica sulle cause dell'incidente e sulle possibili misure di attenuazione.
([2]) Informazioni sulla vulnerabilità tecnica che viene sfruttata per incidere negativamente sui sistemi informatici.

— SEAE:

  — Segretario generale (aggiunto) per la risposta alle crisi e la SIAC (INTCEN dell'UE ed EUMS INT)

  — cellula dell'UE per l'analisi delle minacce ibride

— Consiglio:

  — presidenza (presidente del gruppo orizzontale per le questioni riguardanti il ciberspazio o del Coreper ([1])) con l'assistenza del segretariato generale del Consiglio o del CPS ([2]) e, se attivati, con il sostegno dei dispositivi IPCR.

Conoscenza situazionale

— Assistenza all'elaborazione di relazioni sulla situazione politica/strategica (ad esempio le relazioni ISAA in caso di attivazione dei dispositivi IPCR).

— Il gruppo orizzontale del Consiglio per le questioni riguardanti il ciberspazio prepara le riunioni del Coreper o del CPS, laddove opportuno.

— In caso di attivazione dei dispositivi IPCR,

  — la presidenza può convocare tavole rotonde a sostegno della preparazione delle riunioni del Coreper o del CPS, con la partecipazione dei portatori di interessi negli Stati membri, delle istituzioni, delle agenzie e dei terzi, quali i paesi terzi e le organizzazioni internazionali. Si tratta di riunioni di crisi per individuare le strozzature e presentare proposte di azione per le questioni trasversali,

  — il *servizio capofila della Commissione o il SEAE* in qualità di servizio capofila per l'ISAA elabora la relazione ISAA con i contributi dell'ENISA, della rete dei CSIRT, di Europol/EC3, dell'EUMS INT, dell'INTCEN e di tutti gli altri soggetti coinvolti. La relazione ISAA rappresenta una valutazione che abbraccia l'intera UE, basata sulla correlazione degli incidenti tecnici e della valutazione delle crisi (analisi delle minacce, valutazione dei rischi, conseguenze ed effetti non tecnici, aspetti dell'incidente o della crisi non legati alla cibersicurezza ecc.), adeguata alle esigenze del livello politico e del livello operativo.

— In caso di attivazione dei dispositivi ARGUS,

  — il CERT-UE e l'EC3 ([3]) contribuiscono direttamente allo scambio di informazioni all'interno della Commissione.

— In caso di attivazione del meccanismo di risposta alle crisi del SEAE,

  — la SIAC intensifica la sua raccolta di informazioni, aggrega le informazioni di tutte le fonti ed elabora l'analisi e la valutazione dell'incidente.

Risposta (su richiesta del livello politico)

— Cooperazione transfrontaliera con il punto di contatto unico e le autorità nazionali competenti (direttiva NIS) per attenuare le conseguenze e gli effetti.

— Attivazione di tutte le misure tecniche di attenuazione e coordinamento delle capacità tecniche necessarie per arrestare o ridurre l'impatto degli attacchi sui sistemi informatici bersaglio.

— Cooperazione e, se stabilito, coordinamento delle capacità tecniche verso una risposta comune o collaborativa secondo le ***POS della rete dei CSIRT***.

— Valutazione della necessità di collaborare con terzi pertinenti.

— Processo decisionale nell'ambito della procedura ARGUS (se attivata).

— (se attivati) coordinamento nell'ambito dei dispositivi IPCR (se attivati).

— Sostegno al processo decisionale del SEAE (se attivato), attraverso il meccanismo di risposta alle crisi del SEAE, anche per quanto riguarda i contatti con i paesi terzi e le organizzazioni internazionali, nonché qualsiasi misura volta a tutelare le missioni e le operazioni della PSDC e le delegazioni dell'UE.

([1]) Il Comitato dei rappresentanti permanenti o Coreper (articolo 240 del trattato sul funzionamento dell'Unione europea — TFUE) è responsabile della preparazione dei lavori del Consiglio dell'Unione europea.

([2]) Il comitato politico e di sicurezza è un comitato del Consiglio dell'Unione europea che si occupa della politica estera e di sicurezza comune (PESC) di cui all'articolo 38 del trattato sull'Unione europea.

([3]) In conformità alle condizioni e alle procedure stabilite nel quadro giuridico dell'EC3.

Comunicazioni pubbliche

— Concordare i messaggi pubblici relativi all'incidente.

— Se la crisi comporta una dimensione esterna o di politica di sicurezza e di difesa comune (PSDC), la comunicazione pubblica dovrebbe essere coordinata con il SEAE e il servizio del portavoce dell'AR/VP.

Cooperazione a livello strategico/politico

Soggetti potenziali

— Per gli Stati membri, i ministri responsabili della cibersicurezza

— Per il Consiglio europeo, il presidente

— Per il Consiglio, la presidenza di turno

— In caso di misure nell'ambito del «pacchetto di strumenti della diplomazia informatica», il CPS e il gruppo orizzontale

— Per la Commissione europea, il presidente o il vicepresidente/commissario delegato

— L'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e Vicepresidente della Commissione.

Ambito delle attività: gestione strategica e politica degli aspetti informatici e non della crisi, comprese le misure nell'ambito del quadro relativo a una risposta diplomatica comune dell'UE alle attività informatiche dolose.

Condivisione della conoscenza situazionale

— Individuare le conseguenze delle perturbazioni causate dalla crisi sul funzionamento dell'Unione.

Risposta

— Attivare meccanismi/strumenti supplementari per la gestione delle crisi a seconda della natura e dell'impatto dell'incidente, ad esempio, il meccanismo di protezione civile.

— Adottare misure nell'ambito del quadro per una risposta diplomatica comune dell'UE alle attività informatiche dolose.

— Mettere a disposizione degli Stati membri coinvolti l'assistenza di emergenza, ad esempio attivando il Fondo di risposta alle emergenze cibernetiche ([1]), quando sarà operativo.

— Cooperare e coordinarsi con le organizzazioni internazionali, laddove appropriato, quali le Nazioni Unite (ONU), l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE) e soprattutto la NATO.

— Valutare le implicazioni in materia di difesa e sicurezza nazionale.

Comunicazioni pubbliche

Decidere una strategia di comunicazione comune destinata al pubblico.

RISPOSTA COORDINATA CON GLI STATI MEMBRI A LIVELLO DELL'UE NELL'AMBITO DEI DISPOSITIVI IPCR

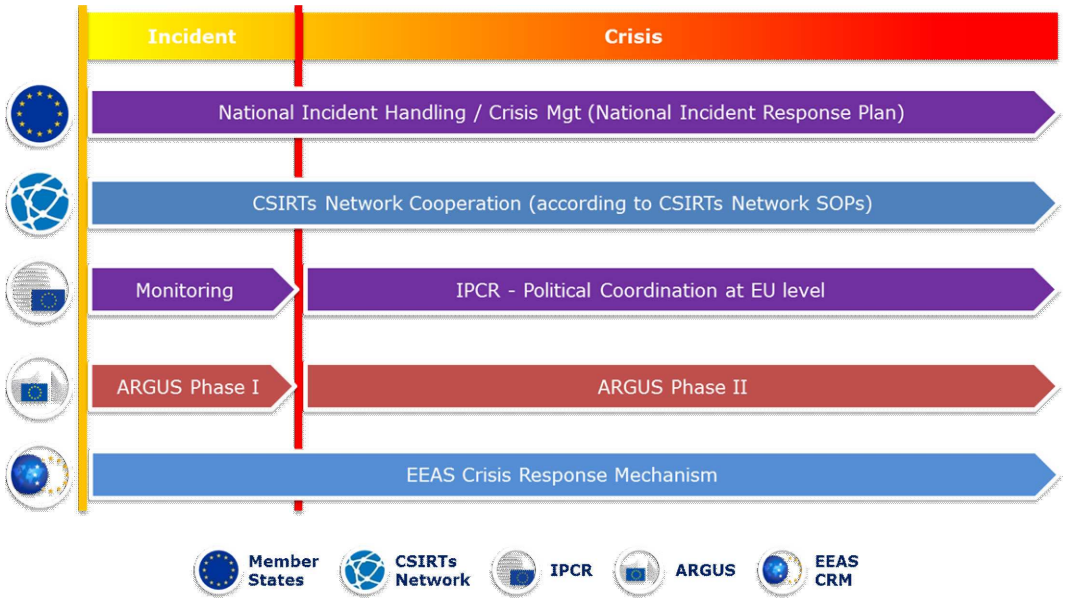
Secondo il principio di complementarità a livello dell'UE, la presente sezione introduce ed esamina nello specifico l'obiettivo, le responsabilità e le attività principali delle autorità degli Stati membri, della rete dei CSIRT, dell'ENISA, di CERT-UE, di Europol/EC3, dell'INTCEN, della cellula dell'UE per l'analisi delle minacce ibride e del gruppo orizzontale del Consiglio per le questioni riguardanti il ciberspazio nell'ambito della procedura IPCR. Si presume che i soggetti agiscano nel rispetto delle procedure stabilite a livello nazionale o dell'UE.

È essenziale notare che, come si evince dalla figura 1, indipendentemente dall'attivazione dei meccanismi di gestione della crisi dell'UE, le attività a livello nazionale e la cooperazione all'interno della rete dei CSIRT (se necessario) durante qualsiasi incidente/crisi si svolgono secondo i principi di sussidiarietà e di proporzionalità.

([1]) Il Fondo di risposta alle emergenze cibernetiche è un'azione proposta nell'ambito della comunicazione congiunta «Resilience, Deterrence and Defence: Building strong cybersecurity for the EU», JOIN(2017) 450/1

Figura 1

Risposta a livello dell'UE in caso di incidente/crisi di cibersicurezza



Tutte le attività descritte di seguito devono essere svolte in conformità e secondo le procedure/norme operative standard dei meccanismi di cooperazione coinvolti e in linea con i mandati e le competenze stabiliti dei singoli soggetti e istituzioni. Tali procedure/norme potrebbero necessitare di alcune integrazioni o modifiche per conseguire la cooperazione migliore possibile e una risposta efficace agli incidenti e alle crisi di cibersicurezza su vasta scala.

Non è sempre necessario che tutti i soggetti indicati di seguito debbano agire in tutti gli incidenti specifici. Tuttavia il programma e le pertinenti procedure operative standard dei meccanismi di cooperazione dovrebbero prevedere il loro eventuale coinvolgimento.

Considerato il diverso grado di impatto che un incidente o una crisi di cibersicurezza possono avere sulla società, occorrerà assicurare un elevato grado di flessibilità per quanto riguarda il coinvolgimento di soggetti settoriali a tutti i livelli e risposte appropriate mediante attività di attenuazione informatiche e non.

Gestione delle crisi di cibersicurezza — Integrare la cibersicurezza nella procedura IPCR

I dispositivi IPCR, descritti nelle POS dell'IPCR ([1]), seguono in ordine di sequenza le fasi descritte di seguito (l'uso di alcune di queste misure dipenderà dalla situazione).

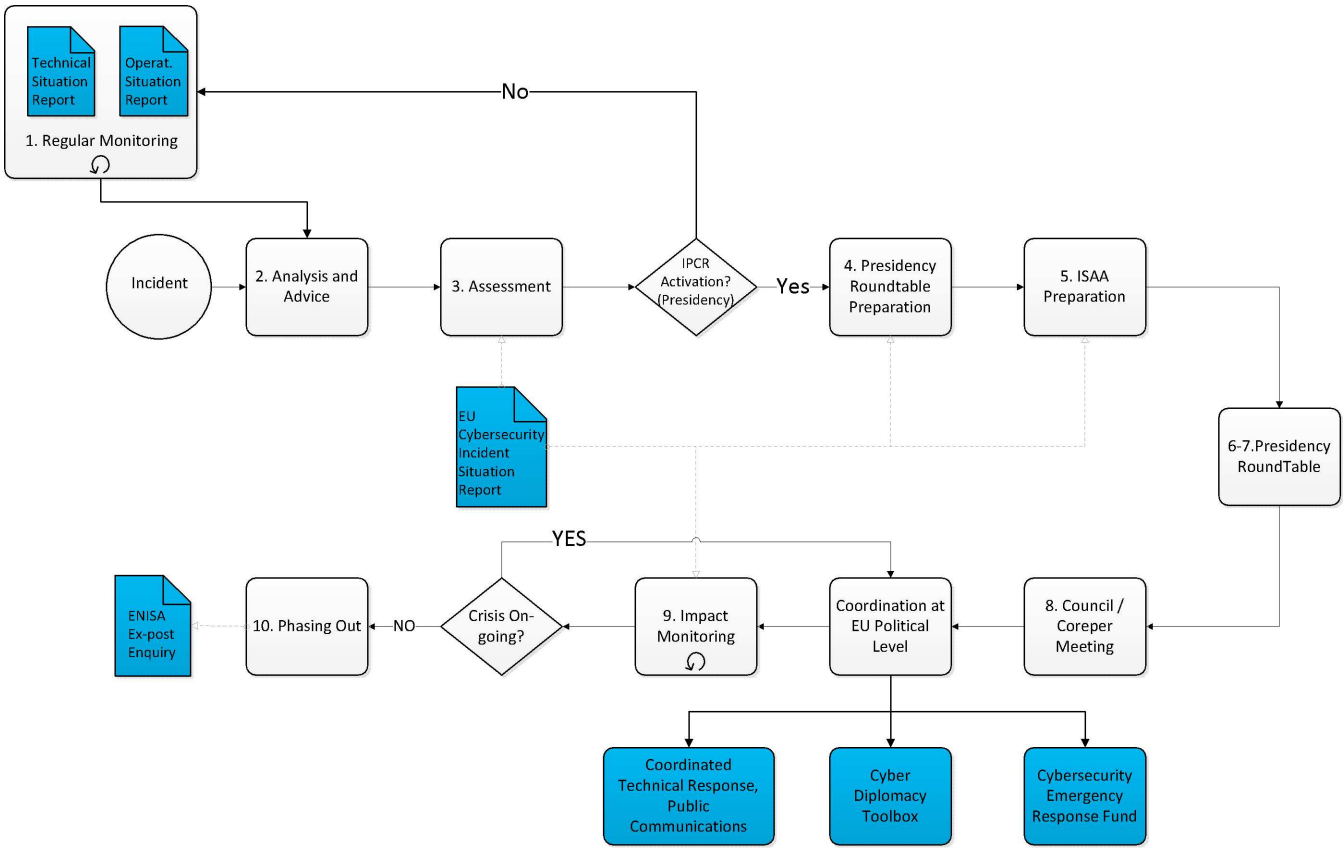
In ciascuna fase sono indicati i soggetti e le attività specifiche per la cibersicurezza. Per facilità di lettura, in ciascuna fase è riportato il testo delle POS dell'IPCR, seguito dalle attività specifiche del programma. Questo approccio fase per fase consente anche una chiara identificazione delle **lacune** esistenti, nelle capacità e nelle procedure necessarie, che ostacolano una risposta efficace alle crisi di cibersicurezza.

La figura 2 (in basso ([2])) è una rappresentazione grafica della procedura dell'IPCR; i nuovi elementi introdotti sono evidenziati in blu.

([1]) Dal documento 12607/15 sulle procedure operative standard dell'IPCR, approvato dal gruppo degli amici della presidenza, di cui il Coreper ha preso nota nell'ottobre 2015.
([2]) Una versione più ampia della figura è riportata in appendice.

Figura 2

Elementi specifici di cibersicurezza nella procedura IPCR



Nota: data la natura delle minacce ibride in ambito cibernetico, che sono destinate a restare al di sotto della soglia di crisi riconoscibile, l'UE deve adottare misure di prevenzione e preparazione. La cellula dell'UE per l'analisi delle minacce ibride è incaricata di analizzare rapidamente gli incidenti rilevanti e di informare le appropriate strutture di coordinamento. Le relazioni periodiche presentate dalla cellula possono contribuire con informazioni utili al processo decisionale settoriale per migliorare la preparazione.

— **Fase 1 — Monitoraggio settoriale periodico e allarmi**. Le relazioni settoriali periodiche sulla situazione e gli allarmi forniscono indicazioni alla presidenza del Consiglio dell'UE sullo sviluppo di una crisi e sulle sue possibili evoluzioni.

  — **Lacuna individuata**: attualmente non sono previsti relazioni periodiche e coordinate sulla situazione e allarmi sugli incidenti (e le minacce) cibernetiche a livello dell'UE.

  — **Programma: monitoraggio/presentazione di relazioni sulla situazione della cibersicurezza nell'UE**

    — L'ENISA elaborerà **una relazione periodica sulla situazione tecnica della cibersicurezza nell'UE** in merito agli incidenti e alle minacce cibernetiche, sulla base delle informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise di CSIRT degli Stati membri (su base volontaria) o dai punti di contatto unici istituiti dalla direttiva NIS, dal Centro europeo per la lotta alla criminalità informatica (EC3) presso Europol, dal CERT-UE e dal Centro dell'UE di analisi dell'intelligence (INTCEN) presso il Servizio europeo per l'azione esterna (SEAE). La relazione dovrebbe essere messa a disposizione delle istanze competenti del Consiglio, della Commissione e della rete dei CSIRT.

    — La cellula dell'UE per l'analisi delle minacce ibride dovrebbe redigere una **relazione sulla situazione operativa della cibersicurezza nell'UE** per conto della SIAC. La relazione è di ausilio anche il quadro per una risposta diplomatica comune dell'UE alle attività informatiche dolose.

    — Entrambe le relazioni sono trasmesse ai portatori di interessi nazionali e dell'UE per contribuire alla loro conoscenza situazionale, informare il processo decisionale e facilitare la cooperazione regionale transfrontaliera.

Dopo l'individuazione di un incidente

— **Fase 2 — Analisi e consulenza**. In base ai dati di monitoraggio e agli allarmi disponibili, i servizi della Commissione, il SEAE e l'SGC si tengono reciprocamente informati sui possibili sviluppi, per essere pronti a fornire una consulenza alla presidenza sull'eventuale attivazione (integrale o in modalità di condivisione delle informazioni) dell'IPCR.

— **Programma**

— Per la Commissione, DG CNECT, DG HOME, DG HR.DS e DG DIGIT con l'assistenza dell'ENISA, dell'EC3 e del CERT-UE.

— SEAE: sulla base del lavoro della SITROOM e delle fonti di intelligence, la cellula dell'UE per l'analisi delle minacce ibride fornisce una conoscenza situazionale delle minacce ibride effettive e potenziali che interessano l'UE e i suoi partner, comprese le minacce cibernetiche. Pertanto, se l'analisi e la valutazione della cellula dell'UE per l'analisi delle minacce ibride indica l'esistenza di possibili minacce contro uno Stato membro, i paesi o le organizzazioni partner, l'INTCEN informerà (in prima istanza) il livello operativo, secondo le procedure stabilite. Il livello operativo elaborerà quindi le raccomandazioni per il livello strategico/politico, tra cui l'eventuale attivazione dei dispositivi di gestione delle crisi in modalità di monitoraggio (ad esempio il meccanismo di risposta alle crisi del SEAE o la pagina di monitoraggio dell'IPCR).

— Il presidente della rete dei CSIRT, assistito dall'ENISA, elabora una relazione sulla situazione degli incidenti di cibersicurezza nell'UE ([1]), che viene presentata alla presidenza, alla Commissione e all'AR/VP attraverso il CSIRT della presidenza di turno.

— **Fase 3 — Valutazione/Decisione in merito all'attivazione dell'IPCR**. La presidenza valuta la necessità di un coordinamento politico, di uno scambio di informazioni o di un processo decisionale a livello dell'UE. A tal fine, la presidenza può convocare una tavola rotonda informale. La presidenza effettua una prima individuazione dei settori che richiedono il coinvolgimento del Coreper o del Consiglio. Ciò costituirà la base degli orientamenti per l'elaborazione delle relazioni sull'analisi e la conoscenza situazionale integrate (Integrated Situational Awareness and Analysis — ISAA). In base alle caratteristiche della crisi, alle sue possibili conseguenze e alle relative esigenze politiche, la presidenza deciderà in merito all'opportunità di convocare riunioni dei pertinenti gruppi di lavoro del Consiglio e/o del Coreper e/o del CPS.

— **Programma**

— Partecipanti alla tavola rotonda:

— i servizi della Commissione e il SEAE forniranno consulenza alla presidenza sui rispettivi settori di competenza;

— i rappresentanti degli Stati membri nel gruppo orizzontale per le questioni riguardanti il ciberspazio, coadiuvati da esperti delle capitali (CSIRT, autorità competenti per la cibersicurezza ecc.);

— orientamento politico/strategico per le relazioni ISAA, in base alla più recente relazione sulla situazione degli incidenti di cibersicurezza nell'UE e alle informazioni aggiuntive fornite dai partecipanti alla tavola rotonda;

— gruppi di lavoro e comitati pertinenti:

— Gruppo orizzontale per le questioni riguardanti il ciberspazio.

La Commissione, il SEAE e l'SGC, in pieno accordo e associandosi alla presidenza, possono inoltre decidere di attivare l'IPCR nella modalità di condivisione delle informazioni mediante la creazione di una pagina di crisi, per preparare il terreno per un'eventuale attivazione completa.

— **Fase 4 — Attivazione dell'IPCR/Raccolta e scambio di informazioni**. In seguito all'attivazione (sia in modalità di condivisione delle informazioni sia completa) viene creata una pagina di crisi sulla piattaforma web dell'IPCR, che consente lo scambio di informazioni specifiche incentrate sugli aspetti che contribuiranno ad alimentare l'ISAA e a preparare la discussione a livello politico. La scelta del servizio capofila per l'ISAA (uno dei servizi della Commissione o il SEAE) dipenderà dalle circostanze del caso.

— **Fase 5 — Elaborazione di relazioni ISAA**. Sarà avviata l'elaborazione di relazioni ISAA. La Commissione/il SEAE pubblicherà relazioni ISAA, come indicato nelle POS ISAA, e potrà favorire ulteriormente lo scambio di

([1]) La relazione sulla situazione degli incidenti di cibersicurezza nell'UE è elaborata aggregando le relazioni nazionali fornite dai CSIRT nazionali. Il formato della relazione dovrebbe essere descritto nelle procedure operative standard (POS) della rete dei CSIRT.

informazioni sulla piattaforma web dell'IPCR o formulare specifiche richieste di informazione. Le relazioni ISAA saranno elaborate per soddisfare le esigenze del livello politico (ossia Coreper o Consiglio), come stabilito dalla presidenza e come indicato nei suoi orientamenti, consentendo in tal modo una visione d'insieme strategica della situazione e un dibattito informato sui punti all'ordine del giorno definiti dalla presidenza. Secondo le POS ISAA, la natura della crisi di cibersicurezza determinerà se la relazione ISAA sarà preparata da uno dei servizi della Commissione (DG CNECT, DG HOME) o dal SEAE.

A seguito dell'attivazione dell'IPCR, la presidenza delineerà gli specifici settori di interesse per l'ISAA al fine di sostenere il coordinamento politico e/o il processo decisionale in seno al Consiglio. La presidenza preciserà anche la data di presentazione della relazione, previa consultazione dei servizi della Commissione e del SEAE.

— **Programma**

— La relazione ISAA comprende contributi dei servizi pertinenti, tra cui:

— la rete dei CSIRT, sotto forma di relazione sulla situazione degli incidenti di cibersicurezza nell'UE;

— l'EC3, la SITROOM, la cellula dell'UE per l'analisi delle minacce ibride e il CERT-UE. La cellula dell'UE per l'analisi delle minacce ibride fornirà sostegno e contributi al servizio capofila per l'ISAA e alla tavola rotonda dell'IPCR, a seconda del caso;

— le agenzie e gli organismi settoriali dell'UE in funzione dei settori colpiti;

— le autorità degli Stati membri (diverse dai CSIRT).

— Raccolta di contributi ISAA ([1]):

— *per la Commissione e le agenzie dell'UE*: il sistema informatico ARGUS costituirà la rete nevralgica interna per l'ISAA. Le agenzie dell'UE invieranno i loro contributi alle rispettive direzioni generali responsabili che, a loro volta, alimenteranno il sistema ARGUS con le informazioni pertinenti. I servizi della Commissione e le agenzie raccoglieranno informazioni dalle reti settoriali già in essere con gli Stati membri e le organizzazioni internazionali e da altre fonti pertinenti;

— *per il SEAE*: la sala situazione dell'UE, con il sostegno degli altri uffici competenti del SEAE, costituirà la rete nevralgica interna e il punto di contatto unico per l'ISAA. Il SEAE raccoglierà informazioni presso i paesi terzi e le organizzazioni internazionali pertinenti.

— **Fase 6 — Preparazione della tavola rotonda informale della presidenza**. La presidenza, assistita dal segretariato generale del Consiglio, definirà la tempistica, l'ordine del giorno, i partecipanti e gli esiti attesi (eventuali risultati tangibili) della tavola rotonda informale della presidenza. Il segretariato generale del Consiglio trasmetterà le informazioni pertinenti alla piattaforma web dell'IPCR a nome della presidenza e, in particolare, pubblicherà la convocazione della riunione.

— **Fase 7 — Tavola rotonda della presidenza/misure preparatorie per il coordinamento politico/il processo decisionale dell'UE**. La presidenza convocherà una tavola rotonda informale per valutare la situazione, nonché preparare ed esaminare gli elementi che devono essere portati all'attenzione del Coreper o del Consiglio. La tavola rotonda informale della presidenza sarà anche la sede per sviluppare, esaminare e discutere tutte le proposte di azione da sottoporre al Coreper/Consiglio.

— **Programma**

— Il gruppo orizzontale del Consiglio per le questioni riguardanti il ciberspazio dovrebbe preparare il comitato politico e di sicurezza (CPS) o il Coreper.

— **Fase 8 — Coordinamento politico e processo decisionale in seno al Coreper/Consiglio**. I risultati delle riunioni del Coreper/delle sessioni del Consiglio riguardano il coordinamento delle attività di risposta a tutti i livelli, le decisioni sulle misure straordinarie, le dichiarazioni politiche ecc. Tali decisioni costituiscono altresì orientamenti politici/strategici aggiornati per l'ulteriore elaborazione di relazioni ISAA.

— **Programma**

— La decisione politica di coordinare la risposta alla crisi di cibersicurezza è attuata mediante le attività (svolte dai soggetti pertinenti), descritte nella precedente sezione 1 «Cooperazione a livello politico/strategico, operativo e tecnico» per quanto riguarda la **risposta** e la **comunicazione pubblica**.

— L'elaborazione di relazioni ISAA continua sulla base della cooperazione a livello tecnico, operativo e politico/strategico per quanto riguarda la **conoscenza situazionale**, anch'essa descritta nella precedente sezione 1.

([1]) POS ISAA

— **Fase 9 — Monitoraggio dell'impatto**. Il servizio capofila per l'ISAA fornirà, con il sostegno di coloro che contribuiscono all'ISAA, informazioni sull'evoluzione della crisi e sull'impatto delle decisioni politiche adottate. Tale ritorno di informazioni sarà alla base di un processo in costante evoluzione, al fine di corroborare la decisione della presidenza di perseverare nel coinvolgimento del livello politico dell'UE o di ridurre il livello di attivazione dell'IPCR.

— **Fase 10 — Graduale cessazione**. Seguendo la stessa procedura già adottata per l'attivazione, la presidenza può convocare una tavola rotonda informale per valutare l'opportunità di mantenere o no attiva l'IPCR. La presidenza può decidere di cessare l'attivazione o di ridurne il livello.

— **Programma**

— L'ENISA potrebbe essere invitata a contribuire o a svolgere un'indagine tecnica ex post dell'incidente in conformità alle disposizioni del suo mandato.

APPENDICE

1. GESTIONE DELLE CRISI, MECCANISMI DI COOPERAZIONE E SOGGETTI A LIVELLO DELL'UE

Meccanismi di gestione delle crisi

Dispositivi integrati per la risposta politica alle crisi (IPCR): i dispositivi integrati per la risposta politica alle crisi (IPCR), approvati dal Consiglio il 25 giugno 2013 ([1]), sono intesi a facilitare un coordinamento e una risposta tempestivi a livello politico dell'UE in caso di grave crisi. L'IPCR sostiene inoltre il coordinamento a livello politico della risposta all'invocazione della clausola di solidarietà (articolo 222 del TFUE), quale definita nella decisione 2014/415/UE del Consiglio relativa alle modalità di attuazione da parte dell'Unione della clausola di solidarietà, adottata il 24 giugno 2014. Le procedure operative standard (POS) dell'IPCR ([2]) stabiliscono la procedura di attivazione e le successive azioni da intraprendere.

ARGUS: sistema di coordinamento in caso di crisi istituito dalla Commissione europea nel 2005 per stabilire una specifica procedura di coordinamento in caso di grave crisi multisettoriale. Esso è sostenuto da un omonimo sistema di allarme rapido (strumento informatico). ARGUS si articola in due fasi, e la fase II (in caso di gravi crisi multisettoriali) comporta la convocazione di riunioni del Comitato di coordinamento di crisi (CCC), sotto l'autorità del presidente della Commissione o di un commissario cui è stata attribuita la responsabilità. Il CCC riunisce i rappresentanti delle pertinenti direzioni generali della Commissione, dei gabinetti e di altri servizi dell'UE al fine di guidare e coordinare la risposta della Commissione alla crisi. Presieduto dal segretario generale aggiunto, il CCC valuta la situazione, esamina le diverse opzioni e adotta decisioni pragmatiche per quanto riguarda gli strumenti dell'UE e gli strumenti di cui è responsabile la Commissione, garantendo l'attuazione delle decisioni adottate ([3]), ([4]).

Meccanismo di risposta alle crisi del SEAE: il meccanismo di risposta alle crisi del SEAE è un sistema strutturato che consente al SEAE di rispondere alle crisi e alle emergenze di natura esterna o con un'importante dimensione esterna, comprese le minacce ibride, che hanno ricadute potenziali o effettive sugli interessi dell'UE o su quelli di qualsiasi Stato membro. Assicurando la partecipazione alle riunioni dei funzionari della Commissione e del segretariato del Consiglio competenti, il meccanismo di risposta alle crisi facilita le sinergie tra gli sforzi diplomatici, di sicurezza e di difesa e gli strumenti finanziari, commerciali e di cooperazione gestiti dalla Commissione. La cellula di crisi può essere attivata per tutta la durata della crisi.

Meccanismi di cooperazione

Rete dei CSIRT: la rete dei CIRST, ossia dei gruppi di intervento per la sicurezza informatica in caso di incidente, riunisce tutti i CSIRT nazionali e governativi e il CERT-UE. Lo scopo della rete è quello di consentire e migliorare la condivisione delle informazioni tra i CSIRT sulle minacce e sugli incidenti di cibersicurezza, nonché cooperare nella risposta alle crisi e agli incidenti nel medesimo settore.

Gruppo orizzontale del Consiglio per le questioni riguardanti il ciberspazio: il gruppo di lavoro è stato istituito per garantire il coordinamento strategico e trasversale, in sede di Consiglio, sulle questioni attinenti alla politica in materia di ciberspazio e può essere coinvolto sia in attività legislative che in attività non legislative.

Soggetti

ENISA: l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, istituita nel 2004, lavora a stretto contatto con gli Stati membri e il settore privato per fornire consulenza e soluzioni su questioni quali le esercitazioni paneuropee per la cibersicurezza, lo sviluppo di strategie nazionali per la cibersicurezza, la creazione delle capacità dei CSIRT e la cooperazione tra gli stessi. L'ENISA collabora direttamente con i CSIRT in tutta l'UE e funge da segretariato della rete dei CSIRT.

ERCC: il centro di coordinamento della risposta alle emergenze della Commissione (nell'ambito della direzione generale per la Protezione civile e le operazioni di aiuto umanitario europee — DG ECHO) sostiene e coordina un'ampia gamma di attività di prevenzione, preparazione e risposta 24 ore su 24, 7 giorni su 7. Inaugurato nel 2013, esso funge da snodo per il sistema di risposta alle crisi della Commissione (in collegamento con le altre cellule di crisi dell'UE) e da punto di contatto centrale dell'IPCR, operativo 24 ore su 24, 7 giorni su 7.

([1]) Documento 10708/13 «Completamento del processo di riesame dei dispositivi di coordinamento nella gestione delle crisi (CCA): dispositivi integrati dell'UE per la risposta politica alle crisi (IPCR)», approvato dal Consiglio il 24 giugno 2013.

([2]) Documento 12607/15 sulle procedure operative standard dell'IPCR, approvato dal gruppo degli amici della presidenza, di cui il Coreper ha preso nota nell'ottobre 2015.

([3]) «Disposizioni della Commissione relative al sistema generale di allarme rapido "ARGUS"» [COM(2005) 662 definitivo del 23 dicembre 2005].

([4]) Decisione 2006/25/CE, Euratom della Commissione, del 23 dicembre 2005, recante modifica del suo regolamento interno (GU L 19 del 24 gennaio 2006, pag. 20), sull'istituzione del sistema generale di allarme rapido «ARGUS».

Europol/EC3: il Centro europeo per la lotta alla criminalità informatica (EC3), istituito nel 2013 nell'ambito di Europol, sostiene l'intervento delle autorità di contrasto nella lotta alla cibercriminalità nell'UE. L'EC3 fornisce agli Stati membri sostegno a livello operativo e di analisi per le indagini e funge da polo di informazione e di intelligence sulla criminalità, sostenendo le operazioni e le indagini degli Stati membri con analisi, coordinamento e competenze a livello operativo, nonché capacità di sostegno a livello tecnico e digitale forense altamente specializzate.

CERT-UE: il gruppo di pronto intervento informatico delle istituzioni, degli organi e delle agenzie europee ha il compito di migliorare la protezione delle istituzioni, degli organi e delle agenzie dell'UE dalle minacce cibernetiche. Esso è membro della rete dei CSIRT. Il CERT-UE ha accordi tecnici sulla condivisione delle informazioni in materia di minacce cibernetiche con la CIRC (capacità di reazione agli incidenti informatici) della NATO, con alcuni paesi terzi e con gli operatori commerciali più importanti nel settore della cibersicurezza.

La comunità dell'intelligence dell'UE comprende il Centro dell'UE di analisi dell'intelligence (**INTCEN**) e la direzione «intelligence» dello Stato maggiore dell'Unione europea (EUMS INT) nel quadro dell'accordo sulla «**capacità unica di analisi dell'intelligence**» (Single Intelligence Analysis Capacity — SIAC). La SIAC ha il compito di fornire analisi d'intelligence, meccanismi di allerta precoce e conoscenza situazionale all'Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza e al Servizio europeo per l'azione esterna (SEAE). La SIAC offre i suoi servizi ai vari organi decisionali dell'UE nei settori della politica estera e di sicurezza comune (PESC), della politica di sicurezza e di difesa comune (PSDC) e della lotta al terrorismo, nonché agli Stati membri. L'INTCEN e l'EUMS INT non sono agenzie operative e non dispongono di capacità di raccolta. Il livello operativo dell'intelligence è di competenza degli Stati membri. La SIAC si occupa unicamente di analisi strategica.

Cellula dell'UE per l'analisi delle minacce ibride: la comunicazione congiunta per contrastare le minacce ibride, dell'aprile 2016, indica la cellula dell'UE per l'analisi delle minacce ibride come punto focale per tutte le analisi delle fonti di minacce ibride nell'UE: il suo mandato è stato approvato nel dicembre 2016 dalla Commissione, a seguito di una consultazione interservizi. Istituita presso l'INTCEN, la cellula dell'UE per l'analisi delle minacce ibride fa parte della SIAC e, di conseguenza, opera congiuntamente all'EUMS INT, con un militare tra i membri permanenti. Il termine «ibrido» fa riferimento a un uso deliberato da parte di uno Stato o di un soggetto non statale di una combinazione di molteplici leve e strumenti palesi o occulti, militari o civili, quali ad esempio i ciberattacchi, le campagne di disinformazione, lo spionaggio, le pressioni economiche, l'uso di forze sussidiarie o altre attività sovversive. La cellula dell'UE per l'analisi delle minacce ibride collabora con un'ampia rete di punti di contatto, sia all'interno della Commissione che negli Stati membri, per fornire la risposta integrata/l'approccio governativo a tutto tondo necessari per rispondere a sfide di varia natura.

SITROOM dell'UE: la sala situazione dell'UE fa parte del Centro dell'UE di analisi dell'intelligence (INTCEN) e fornisce al SEAE la capacità operativa per garantire una risposta immediata ed efficace alle crisi. Si tratta di un organismo permanente civile-militare di pronto intervento, che svolge attività di monitoraggio e di conoscenza situazionale mondiali ed è operativo 24 ore su 24, 7 giorni su 7.

Strumenti pertinenti

Quadro per una risposta diplomatica comune dell'UE alle attività informatiche dolose: approvato nel giugno 2017, il quadro fa parte dell'approccio dell'UE alla diplomazia informatica, che contribuisce a prevenire i conflitti, a ridurre le minacce alla cibersicurezza e a incrementare la stabilità nelle relazioni internazionali. Il quadro si avvale pienamente delle misure della politica estera e di sicurezza comune, anche di misure restrittive, laddove necessario. Il ricorso alle misure nel contesto del quadro dovrebbe incoraggiare la cooperazione, facilitare l'attenuazione delle minacce immediate e a lungo termine e influenzare il comportamento degli autori delle minacce e dei potenziali aggressori nel lungo periodo.

2. COORDINAMENTO DELLE CRISI DI CIBERSICUREZZA NEI DISPOSITIVI IPCR — COORDINAMENTO ORIZZONTALE E ATTIVAZIONE POLITICA

I dispositivi IPCR possono essere (e sono stati) usati per affrontare questioni tecniche e operative, ma sempre da un punto di vista politico/strategico.

In termini di attivazione, l'IPCR può essere utilizzata in funzione del livello della crisi, passando dalla «modalità monitoraggio» alla «modalità condivisione di informazioni», che è il primo livello di attivazione dell'IPCR, fino all'«attivazione completa dell'IPCR».

L'attivazione completa del meccanismo è una decisione della presidenza di turno del Consiglio dell'UE. La «modalità condivisione di informazioni» dell'IPCR può essere attivata dalla Commissione, dal SEAE e dal segretariato generale del

Consiglio. Il monitoraggio e la condivisione di informazioni innescano livelli differenti di scambio di informazioni: la «modalità condivisione di informazioni» attiva la richiesta di elaborare relazioni ISAA. L'attivazione completa aggiunge, agli strumenti disponibili, le riunioni della tavola rotonda dell'IPCR, portando al tavolo delle riunioni la presidenza (di norma, il presidente del Coreper II o un esperto della materia a livello di consigliere della rappresentanza permanente ma, in via eccezionale, si sono tenute tavole rotonde a livello ministeriale).

Soggetti

La presidenza di turno (di solito il presidente del Coreper) fa da capofila;

per il Consiglio europeo, il gabinetto del presidente;

per la Commissione europea, funzionari al livello del segretario generale aggiunto/di direttore generale e/o esperti della materia;

per il SEAE, funzionari al livello del segretario generale aggiunto/di direttore esecutivo e/o esperti della materia;

per il segretariato generale del Consiglio, il gabinetto del segretario generale, il gruppo dell'IPCR e le DG responsabili.

Ambito delle attività: tracciare un quadro integrato comune della situazione e attivare la conoscenza delle strozzature e delle carenze a ciascuno dei tre livelli, al fine di affrontarle sul piano politico, produrre decisioni al tavolo delle riunioni, se rientrano nella sfera di competenza dei partecipanti, o produrre proposte d'azione destinate al Coreper II e successivamente al Consiglio.

Condivisione della conoscenza situazionale

(Non attiva): possono essere generate pagine di monitoraggio dell'IPCR per seguire lo sviluppo di situazioni che potrebbero degenerare in una crisi con implicazioni nell'UE;

(modalità condivisione di informazioni dell'IPCR): le relazioni ISAA saranno elaborate dal capofila dell'ISAA sulla base del contributo dei servizi della Commissione, del SEAE e degli Stati membri (tramite i questionari IPCR);

(modalità attivazione completa dell'IPCR): oltre alle relazioni ISAA, tavole rotonde informali dell'IPCR riuniscono i diversi soggetti interessati negli Stati membri, la Commissione, il SEAE, le agenzie pertinenti ecc. al fine di discutere le carenze e le strozzature.

Cooperazione e risposta

Attivare/sincronizzare meccanismi/strumenti supplementari per la gestione delle crisi, a seconda della natura e dell'impatto dell'incidente, che possono comprendere, ad esempio, il meccanismo di protezione civile, il quadro per una risposta diplomatica comune dell'UE alle attività informatiche dolose o il «Quadro congiunto per contrastare le minacce ibride».

Comunicazioni in caso di crisi

La rete dei comunicatori dell'IPCR in caso di crisi può essere attivata dalla presidenza, previa consultazione dei pertinenti servizi della Commissione, del segretariato generale del Consiglio e del SEAE, al fine di sostenere la creazione di messaggi comuni o di sviluppare gli strumenti di comunicazione più efficaci.

3. GESTIONE DELLE CRISI DI CIBERSICUREZZA NEL SISTEMA ARGUS — CONDIVISIONE DELLE INFORMAZIONI ALL'INTERNO DELLA COMMISSIONE EUROPEA

Di fronte alle crisi impreviste per le quali è stata necessaria un'azione a livello europeo, ad esempio gli attentati terroristici di Madrid (marzo 2004), lo tsunami in Asia sudorientale (dicembre 2004) e gli attacchi terroristici di Londra (luglio 2005), nel 2005 la Commissione ha istituito il sistema di coordinamento ARGUS che, sostenuto dall'omonimo sistema generale di allarme rapido ([1]), ([2]), è inteso a stabilire una specifica **procedura di coordinamento** in caso di grave crisi multisettoriale, per consentire la condivisione in tempo reale di informazioni riguardanti la crisi e garantire la rapidità del processo decisionale.

ARGUS prevede due fasi, a seconda della gravità dell'evento.

Fase I: è utilizzata per la «condivisione di informazioni» durante una crisi di portata limitata.

([1]) Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni Disposizioni della Commissione relative al sistema generale di allarme rapido «ARGUS» [COM(2005) 662 definitivo del 23 dicembre 2005].

([2]) Decisione 2006/25/CE, Euratom.

Esempi di eventi recenti del tipo «fase I» segnalati comprendono gli incendi boschivi in Portogallo e Israele, l'attacco di Berlino del 2016, le inondazioni in Albania, l'uragano Matthew ad Haiti e la siccità in Bolivia. Qualsiasi DG può aprire un evento del tipo «fase I», nel caso in cui ritenga che la situazione nel suo settore di competenza sia sufficientemente grave da giustificare o trarre beneficio dalla condivisione di informazioni. Ad esempio, la DG CNECT o la DG HOME possono aprire un evento del tipo «fase I» nel caso in cui ritengano che una situazione connessa alla cibersicurezza nei loro rispettivi settori di competenza sia sufficientemente grave da giustificare o trarre beneficio dalla condivisione di informazioni.

Fase II: è attivata in caso di grave crisi multisettoriale ovvero di minaccia prevedibile o imminente per l'Unione.

La fase II comporta una specifica procedura di coordinamento che consente alla Commissione di prendere decisioni e gestire una risposta rapida, coordinata e coerente al più alto livello nel suo settore di competenza e in cooperazione con le altre istituzioni. La fase II è destinata alle situazioni di grave crisi multisettoriale ovvero di minaccia prevedibile o imminente. Tra gli esempi di eventi reali del tipo «fase II» figurano la crisi dei rifugiati/della migrazione (dal 2015 a tutt'oggi), la triplice catastrofe di Fukushima (2011) e l'eruzione del vulcano Eyjafjallajökull in Islanda (2010).

La fase II è attivata dal presidente, di propria iniziativa o su richiesta di un membro della Commissione. Il presidente può attribuire al commissario responsabile del servizio maggiormente interessato dalla crisi in atto la responsabilità politica dell'intervento della Commissione o assumere egli stesso tale responsabilità.

La fase II prevede riunioni d'urgenza del Comitato di coordinamento di crisi (CCC) che sono indette sotto l'autorità del presidente o del commissario al quale è stata attribuita la responsabilità. Le riunioni sono convocate dal segretariato generale mediante lo strumento informatico ARGUS. Il CCC è una struttura operativa specifica per la gestione delle crisi, istituita al fine di dirigere e coordinare l'intervento della Commissione in caso di crisi, che riunisce le DG della Commissione, i gabinetti e gli altri servizi dell'UE competenti. Presieduto dal segretario generale aggiunto, **il CCC valuta la situazione, esamina le diverse opzioni e adotta decisioni, e garantisce l'attuazione delle decisioni e dei provvedimenti** e, nel contempo, la coerenza e l'uniformità dell'intervento. Il sostegno al CCC è fornito dal segretariato generale.

4. MECCANISMO DI RISPOSTA ALLE CRISI DEL SEAE

Il meccanismo di risposta alle crisi del SEAE è attivato nel caso di una situazione grave o di emergenza che riguarda o comunque coinvolge la dimensione esterna dell'UE. Il meccanismo è attivato dal segretario generale aggiunto per la risposta alle crisi, previa consultazione dell'AR/VP o del segretario generale. Anche l'AR/VP, l'SG, un altro segretario generale aggiunto o il direttore esecutivo possono chiedere al segretario generale aggiunto di avviare il meccanismo di risposta alle crisi.

Esso contribuisce alla coerenza dell'UE nella risposta alle crisi nel quadro della strategia per la sicurezza. In particolare, tale meccanismo facilita le sinergie tra gli sforzi diplomatici, di sicurezza e di difesa e gli strumenti finanziari, commerciali e di cooperazione gestiti dalla Commissione.

Esso è collegato al sistema generale di risposta alle emergenze della Commissione (ARGUS) e ai dispositivi dell'IPCR, al fine di sfruttare le sinergie in caso di attivazione simultanea. La sala situazione del SEAE funge da polo di comunicazione tra il SEAE e i sistemi di risposta alle emergenze del Consiglio e della Commissione.

Di norma, la prima azione connessa all'attuazione del meccanismo è la convocazione di una **riunione di crisi** tra gli alti dirigenti del SEAE, della Commissione e del Consiglio direttamente interessati dalla crisi in questione. Durante la riunione di crisi si valutano gli effetti a breve termine della crisi e si possono concordare provvedimenti immediati oppure l'attivazione della cellula di crisi o la convocazione di una piattaforma di crisi. Tali azioni possono essere attuate in qualsiasi sequenza temporale.

La **cellula di crisi** è una sala operativa su scala ridotta in cui i rappresentanti dei servizi del SEAE, della Commissione e del Consiglio coinvolti nella risposta alla crisi si riuniscono per monitorare la situazione in modo continuativo al fine di fornire sostegno ai decisori che operano presso la sede centrale del SEAE. Quando viene attivata, la cellula di crisi è operativa 24 ore su 24, 7 giorni su 7.

La **piattaforma di crisi** riunisce i servizi pertinenti del SEAE, della Commissione e del Consiglio per valutare a medio e lungo termine gli effetti delle crisi e concordare le azioni da intraprendere. Essa è presieduta dall'AR/VP o dal segretario generale o dal segretario generale aggiunto per la risposta alle crisi. La piattaforma di crisi valuta l'efficacia dell'azione dell'UE nel paese o nella regione in situazione di crisi, decide le modifiche alle misure supplementari e discute le proposte di azione del Consiglio. La piattaforma di crisi è una riunione ad hoc, pertanto non è attivata in modo permanente.

La **task force** è composta da rappresentanti dei servizi coinvolti nell'intervento e può essere attivata per seguire e facilitare l'attuazione dell'intervento dell'UE. Essa valuta l'impatto dell'azione dell'UE, elabora documenti politici e documenti di opzioni, contribuisce alla preparazione del quadro politico per l'approccio alle crisi (PFCA), contribuisce alla strategia di comunicazione e adotta qualsiasi altro dispositivo in grado di agevolare l'attuazione dell'intervento dell'UE.

5. DOCUMENTI DI RIFERIMENTO

In appresso figura un elenco dei documenti di riferimento che sono stati presi in considerazione nella preparazione del programma:

— «European Cyber Crises Cooperation Framework», versione 1 del 17 ottobre 2012.

— «Report on Cyber Crisis Cooperation and Management», ENISA, 2014

— «Actionable Information for Security Incident Response», ENISA, 2014

— «Common practices of EU-level crisis management and applicability to cyber crises», ENISA, 2015

— «Strategies for Incident Response and Cyber Crisis Cooperation», ENISA, 2016

— «EU Cyber Standard Operating Procedures», ENISA, 2016

— «A good practice guide of using taxonomies in incident prevention and detection», ENISA, 2017

— Comunicazione della Commissione «Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza» (COM(2016) 410 final del 5.7.2016).

— «Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza» — conclusioni del Consiglio del 15 novembre 2016, documento 14540/16

— Decisione 2014/415/UE del Consiglio, del 24 giugno 2014, relativa alle modalità di attuazione da parte dell'Unione della clausola di solidarietà (GU L 192 dell'1.7.2014, pag. 53)

— «Completamento del processo di riesame dei dispositivi di coordinamento nella gestione delle crisi (CCA): i dispositivi integrati dell'UE per la risposta politica alle crisi (IPCR)», documento 10708/13 del 7 giugno 2013.

— «Integrated Situational Awareness and Analysis (ISAA) — Standard Operating Procedures», DS 1570/15 del 22 ottobre 2015.

— «Disposizioni della Commissione relative al sistema generale di allarme rapido "ARGUS"» (COM(2005) 662 definitivo del 23 dicembre 2005).

— Decisione 2006/25/CE, Euratom della Commissione, del 23 dicembre 2005, recante modifica del suo regolamento interno (GU L 19 del 24 gennaio 2006, pag. 20).

— Modus Operandi di ARGUS, Commissione europea, 23 ottobre 2013

— «Progetto di conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica")», documento 9916/17

— «EU operational protocol for countering hybrid threats "EU Playbook"», SWD(2016) 227 final

— Meccanismo di risposta alle crisi del SEAE dell'8 novembre 2016 [Ares(2017)880661]. Documento di lavoro congiunto dei servizi «EU operational protocol for countering hybrid threats EU Playbook» [SWD(2016) 227 final del 5 luglio 2016]

— Comunicazione congiunta al Parlamento europeo e al Consiglio «Quadro congiunto per contrastare le minacce ibride — La risposta dell'Unione europea» [JOIN(2016) 18 final del 6 aprile 2016].

— Documento di lavoro del Servizio europeo per l'azione esterna «EU Hybrid Fusion Cell — Terms of Reference» [EEAS(2016) 1674].

6. ELEMENTI SPECIFICI DELLA CIBERSICUREZZA NELLA PROCEDURA IPCR