Consiglio
dell'Unione europea

Bruxelles, 10 dicembre 2021
(OR. en)

14874/21

JAI 1390	**DROIPEN 155**
COSI 247	**COPEN 448**
ENFOPOL 503	**FREMP 294**
ENFOCUSTOM 192	**JAIEX 133**
IXIM 287	**CFSP/PESC 1223**
CT 171	**COPS 465**
CRIMORG 161	**HYBRID 79**
FRONT 434	**DISINFO 44**
ASIM 102	**TELECOM 458**
VISA 249	**DIGIT 186**
CYBER 327	**COMPET 899**
DATAPROTECT 284	**RECH 558**
CATS 79	

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	8 dicembre 2021
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, segretario generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2021) 799 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO sulla terza relazione sui progressi compiuti nell'attuazione della strategia dell'UE per l'Unione della sicurezza

Si trasmette in allegato, per le delegazioni, il documento COM(2021) 799 final.

All.: COM(2021) 799 final

COMMISSIONE
EUROPEA

Bruxelles, 8.12.2021
COM(2021) 799 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

sulla terza relazione sui progressi compiuti nell'attuazione della strategia dell'UE per l'Unione della sicurezza

I. Introduzione

L'Unione della sicurezza mira a garantire che l'UE svolga appieno il suo ruolo nel garantire la sicurezza dei cittadini nel rispetto dei valori che definiscono lo stile di vita europeo. L'attuazione sta procedendo in relazione a tutte e quattro le priorità strategiche definite nella strategia per l'Unione della sicurezza[1]: i) un ambiente della sicurezza adeguato alle esigenze del futuro; ii) affrontare le minacce in evoluzione; iii) proteggere gli europei dal terrorismo e dalla criminalità organizzata; e iv) un forte ecosistema europeo della sicurezza.

La pandemia di COVID-19 ha accentuato le principali vulnerabilità, mentre le minacce e le sfide per la sicurezza europea continuano a evolvere in risposta alle trasformazioni tecnologiche e agli sviluppi internazionali. La seconda relazione sull'Unione della sicurezza[2] illustra le particolari sfide per la sicurezza presentate dalla pandemia di COVID-19.

La presente terza relazione si concentra sugli sviluppi degli ultimi sei mesi connessi alle principali minacce emergenti in questo periodo. Sottolinea in particolare la necessità di intensificare la cooperazione non solo all'interno dell'UE, ma anche a livello internazionale, con un'ampia gamma di portatori di interessi e partner.

La strategia per l'Unione della sicurezza è portata avanti nel contesto di minacce sempre più transfrontaliere e intersettoriali. Il mondo digitale continua a essere sfruttato a fini dolosi. Gli attacchi informatici che hanno origine all'interno o all'esterno dell'Europa, compresi gli attacchi ransomware, sono sempre più frequenti e colpiscono le funzioni essenziali dello Stato, quali l'assistenza sanitaria e le infrastrutture fondamentali, le industrie e gli enti pubblici, nonché i singoli individui. Le attività di manipolazione delle informazioni e le ingerenze straniere sono in aumento e in alcuni casi sono andate di pari passo con le attività informatiche, in particolare le operazioni di hack-and-leak. La criminalità organizzata di ogni tipo continua a operare a livello transfrontaliero e per una risposta efficace servono partenariati al di fuori dell'UE. Gli sviluppi internazionali richiedono una vigilanza nel contesto di una potenziale radicalizzazione e terrorismo, nonché di attacchi ibridi anche, durante il periodo di riferimento, alle frontiere esterne dell'UE.

Per far fronte a queste minacce sempre più sofisticate a livello mondiale e transfrontaliero, l'UE sta intensificando non solo la propria capacità di risposta, ma anche la cooperazione con i partner internazionali. Questo è un tema centrale della presente relazione.

Nel contempo si stanno intensificando i lavori per rafforzare la sicurezza nello spazio Schengen. Una stretta cooperazione tra gli Stati membri è fondamentale per la sicurezza generale dello spazio Schengen. Per apportare ulteriori miglioramenti al riguardo, la Commissione ha preparato un nuovo e sostanziale pacchetto comprendente misure volte a rafforzare la cooperazione di polizia e la sicurezza dello spazio Schengen.

Le agenzie dell'UE sono pienamente coinvolte in questi lavori attraverso le loro attività operative a sostegno delle autorità nazionali degli Stati membri, nonché attraverso la messa a disposizione di competenze, informazioni e conoscenza situazionale sulle minacce più urgenti.

Ulteriori dettagli e aggiornamenti sull'intera gamma di iniziative nell'ambito dell'Unione della sicurezza sono presentati in un allegato della presente comunicazione.

---

[1] COM(2020) 605 final.
[2] COM(2021) 440 final.

II. Un ambiente della sicurezza adeguato alle esigenze del futuro

Le infrastrutture digitali, le tecnologie e i sistemi online ci consentono di creare attività imprenditoriali, consumare prodotti e usufruire di servizi. Tuttavia questa crescente digitalizzazione del nostro ambiente ci rende anche più vulnerabili agli attacchi. La portata, la frequenza e la sofisticazione della criminalità informatica e degli attacchi informatici sono in aumento, secondo la valutazione della minaccia della criminalità organizzata su internet pubblicata da **Europol** nel novembre 2021[3] e la relazione annuale dell'Agenzia dell'UE per la cibersicurezza (**ENISA**) sul panorama delle minacce dell'ottobre 2021. Nell'ultimo anno i governi europei si sono trovati ad affrontare almeno 198 incidenti di cibersicurezza, il che ha reso la pubblica amministrazione il settore più pesantemente colpito. I responsabili degli attacchi sono malintenzionati altamente qualificati e dotati di risorse adeguate provenienti dall'interno dell'UE, ma anche da paesi terzi, che sfruttano la natura "senza frontiere" della rete internet globale e aperta e le lacune giurisdizionali dei quadri attuali. Gli attacchi informatici e la criminalità informatica sono spesso interconnessi, come dimostrato da numerosi incidenti in cui i criminali prendono di mira le vulnerabilità per estorcere denaro, e costituiscono una minaccia costante e in continua evoluzione. I criminali informatici possono essere motivati semplicemente dalle crescenti opportunità di monetizzazione delle loro attività, ma altri comportamenti dolosi da parte di soggetti statali o non statali sono motivati da considerazioni geopolitiche e ideologiche più complesse, oltre che da vantaggi finanziari. I dati raccolti dall'**ENISA** hanno dimostrato che gli hacker sostenuti dallo Stato hanno raggiunto anche "nuovi livelli di sofisticazione e impatto" con attacchi contro le catene di approvvigionamento del settore pubblico e privato[4].

È quindi particolarmente importante mantenere un elevato livello di ambizione per l'azione dell'UE, sia per quanto riguarda il livello di sicurezza che intendiamo raggiungere che per quanto riguarda il ritmo di lavoro con cui ci adopereremo per conseguirlo. Il Consiglio europeo dell'ottobre 2021[5] ha affrontato il problema del consistente aumento delle attività informatiche dolose. Ha ribadito l'impegno dell'UE a favore di un ciberspazio aperto, libero, stabile e sicuro e ha sottolineato la necessità di un coordinamento e di una preparazione efficaci di fronte alle crescenti minacce alla cibersicurezza. Ha inoltre posto l'accento sulla necessità di intensificare l'azione nella lotta contro la criminalità informatica, in particolare contro gli attacchi ransomware, e di rafforzare la cooperazione con i paesi partner, anche nei consessi multilaterali.

---

3 Valutazione della minaccia della criminalità organizzata su internet, 11 novembre 2021.
4 Relazione annuale ENISA sul panorama delle minacce, 27 ottobre 2021.
5 Conclusioni del Consiglio europeo, 21-22 ottobre 2021.

Alcuni esempi di recenti incidenti informatici/ransomware nel periodo di riferimento

- Luglio: circa 500 supermercati in Svezia sono stati costretti a chiudere a causa di un attacco informatico molto aggressivo che ha colpito organizzazioni di tutto il mondo.
- Luglio: l'**Estonia** ha riferito che un hacker con sede a Tallinn ha scaricato 286 438 foto identificative dalle banche dati governative, mettendo in luce una vulnerabilità in una piattaforma gestita dall'autorità del sistema informativo.
- Agosto: la regione Lazio in **Italia** ha subito un attacco ransomware che ha disattivato i sistemi informatici amministrativi, compreso il portale di registrazione per la vaccinazione contro la COVID-19. Per diversi giorni dopo l'attacco non è stato possibile programmare nuovi appuntamenti per la vaccinazione.
- Settembre: in **Germania** è stato confermato un attacco informatico in cui gli hacker sono riusciti a violare i sistemi di server e file dell'Ufficio federale di statistica tedesco, che è guidato dal commissario elettorale nazionale.
- Settembre: nei **Paesi Bassi**, un attacco informatico ha ostacolato l'avvio di un passaporto COVID.
- Ottobre: un attacco ransomware contro un ospedale in **Belgio** ha costretto quest'ultimo ad annullare tutte le visite programmate.
- Novembre: durante l'attacco informatico al ramo europeo di Mediamarkt, gli hacker hanno chiesto 50 milioni di USD in bitcoin.

Affrontare la resilienza dell'UE a livello interno

Le proposte della Commissione del 2020 sulla **protezione e la resilienza delle infrastrutture critiche**, sia fisiche che digitali, sono attualmente in corso di negoziazione al Parlamento europeo e al Consiglio. Il 19 ottobre 2021 il Parlamento ha adottato il suo mandato negoziale per il progetto di direttiva sulla resilienza dei soggetti critici e il 10 novembre 2021 per il progetto di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS 2). Il 3 dicembre il Consiglio ha raggiunto un orientamento generale sulla direttiva NIS 2. Ciò aprirà la strada a una conclusione rapida, coerente e ambiziosa dei negoziati nel 2022.

Una componente fondamentale per aumentare la capacità dell'UE di reagire e riprendersi rapidamente è stata la raccomandazione della Commissione di istituire un'**unità congiunta per il ciberspazio**. Tale unità riunirà gli Stati membri e le istituzioni, le agenzie e gli organismi competenti dell'UE per fornire una struttura per una cooperazione coordinata a livello operativo. Essa contribuirebbe a collegare i vari attori responsabili delle operazioni di cibersicurezza nelle comunità della cibersicurezza dell'UE (resilienza, attività di contrasto, diplomazia informatica e ciberdifesa). Il 19 ottobre il Consiglio ha convenuto[6] di esplorare il potenziale dell'iniziativa relativa all'unità congiunta per il ciberspazio a complemento della raccomandazione della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala. È stato avviato un processo preparatorio e l'**ENISA** ha organizzato diversi seminari per discutere i risultati tangibili e le prossime tappe, quali

[6] Conclusioni del Consiglio — Esplorare il potenziale dell'iniziativa concernente un'unità congiunta per il ciberspazio a integrazione della risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala, 12534/2021, https://data.consilium.europa.eu/doc/document/ST-12534-2021-INIT/it/pdf.

definiti nella raccomandazione della Commissione e tenendo conto del documento della presidenza slovena sul percorso da seguire per l'unità congiunta per il ciberspazio[7].

Oltre a tali proposte generali, la legislazione settoriale integra questi lavori tenendo conto delle vulnerabilità specifiche, e durante il periodo di riferimento si possono osservare progressi nei settori finanziario, sanitario, marittimo ed energetico e nella protezione dei consumatori.

Stanno procedendo i negoziati sull'**atto sulla resilienza operativa digitale per il settore finanziario**, che mira a rafforzare la resilienza operativa digitale complessiva degli istituti finanziari. Il Consiglio ha raggiunto un orientamento generale il 24 novembre, mentre il Parlamento europeo intende adottare il suo mandato negoziale entro la fine dell'anno. Una volta adottate, tali misure forniranno all'UE e ai suoi Stati membri un quadro legislativo solido e adeguato alle esigenze del futuro per affrontare tali sfide in modo più efficace, a condizione che il livello di ambizione richiesto si rifletta nell'esito finale dei negoziati.

La pandemia è servita a sottolineare la natura fondamentale del settore sanitario e la necessità di un solido quadro di **sicurezza sanitaria**. Le proposte relative all'Unione europea della salute mirano a migliorare la protezione, la prevenzione, la preparazione e la risposta nei confronti dei rischi per la salute umana a livello dell'UE e dimostrano l'ambizione e la determinazione dell'UE per quanto riguarda la protezione di questo settore essenziale. È già stato raggiunto un accordo sull'aggiornamento dei mandati delle principali agenzie e presto dovrebbe seguirne uno sulle minacce sanitarie transfrontaliere. Anche l'avvio, nel settembre 2021, dell'Autorità dell'UE per la preparazione e la risposta alle emergenze sanitarie (HERA) ha aggiunto una nuova dimensione a questi lavori e sarà sostenuto da un nuovo quadro di misure di emergenza limitate nel tempo, da attivare se necessario.

Le minacce ibride e informatiche nel settore marittimo, rivolte a **infrastrutture marittime** critiche quali porti, cavi e condutture sottomarini, piattaforme energetiche e punti di strozzatura del traffico marittimo, possono essere estremamente destabilizzanti. La strategia per la sicurezza marittima dell'UE e il relativo piano d'azione[8] sono attualmente in fase di valutazione ai fini di un eventuale aggiornamento, attraverso il quale l'evoluzione delle minacce ibride e informatiche potrebbe essere affrontata in modo più efficace.

Nella recente comunicazione "Risposta all'aumento dei prezzi dell'**energia**: un pacchetto di misure d'intervento e di sostegno"[9], la Commissione ha annunciato l'intenzione di intraprendere azioni entro la fine del 2022 per adattare la resilienza del sistema energetico alle nuove minacce, come gli attacchi informatici o gli eventi meteorologici estremi, tra cui nuove norme sulla cibersicurezza dell'energia elettrica, una raccomandazione sugli aspetti relativi alla resilienza dell'energia pulita e un gruppo europeo permanente di operatori e autorità sulla resilienza delle infrastrutture energetiche.

Le vulnerabilità in materia di sicurezza sono presenti anche in molti prodotti intelligenti e dispositivi senza fili. In particolare i bambini possono essere esposti a rischi per la sicurezza a

---

[7] La presidenza slovena ha inoltre elaborato un documento di lavoro (13019/21) sul percorso da seguire per l'unità congiunta per il ciberspazio, che delinea misure concrete per rafforzare la conoscenza situazionale comune tra le comunità informatiche pertinenti e al loro interno.

[8] Relazione sull'attuazione del piano d'azione riveduto della strategia per la sicurezza marittima dell'UE (SWD(2020) 252 final).

[9] COM(2021) 660 final.

causa delle vulnerabilità dei **prodotti elettronici**, come i giocattoli connessi e gli smartwatch. Per affrontare la questione, nell'ottobre 2021 la Commissione ha adottato un atto delegato a norma della direttiva sulle apparecchiature radio per proteggere la vita privata e le reti e per tutelare dalle frodi nei prodotti elettronici connessi[10]. Ciò imporrebbe ai fabbricanti obblighi che aumenterebbero il livello di cibersicurezza dei prodotti immessi sul mercato dell'UE e consentirebbe agli Stati membri di adottare misure correttive qualora vengano trovati sul mercato prodotti non sicuri.

Affrontare la resilienza dell'UE attraverso la cooperazione internazionale

Le minacce alla sicurezza sono di natura mondiale e la creazione di solidi partenariati internazionali è essenziale per affrontarle in modo efficace. L'UE e i suoi Stati membri stanno pertanto intensificando la loro azione per prevenire, scoraggiare e affrontare le minacce da parte di soggetti statali e non statali, anche attraverso sforzi volti ad attribuire più chiaramente la responsabilità. Nel luglio 2021, l'UE[11], gli Stati Uniti, la NATO e altre potenze mondiali hanno rilasciato dichiarazioni che denunciavano con forza le attività informatiche dolose e attribuivano al territorio cinese l'hackeraggio dei server di Microsoft Exchange dell'inizio del 2021. Questa attività informatica dolosa ha compromesso oltre 100 000 server in tutto il mondo. Il 24 settembre 2021, l'alto rappresentante ha rilasciato una dichiarazione a nome dell'UE[12] sul rispetto dei processi democratici dell'UE, denunciando una serie di attività informatiche dolose, esortando la Federazione russa a rispettare le norme del comportamento responsabile degli Stati nel ciberspazio e chiedendo a tutte le parti coinvolte di porre fine immediatamente a tale attività.

Le discussioni sulle sfide globali in materia di sicurezza si stanno intensificando a livello **multilaterale**. Nella riunione dei ministri degli Interni e della Sicurezza del **G7** del settembre 2021 è stata discussa una serie di questioni che spaziano dal materiale pedopornografico online agli attacchi ransomware, alla lotta contro il terrorismo e le forme gravi di criminalità, fino alla corruzione. I partner del G7 hanno condiviso posizioni convergenti e si sono impegnati ad aumentare lo scambio di informazioni (compresi dati biometrici e biografici), garantendo nel contempo la protezione dei dati personali e dei diritti fondamentali.

L'UE ha inoltre partecipato alla riunione dei ministri del Digitale del **G20** tenutasi nel mese di agosto sotto la presidenza italiana. I ministri hanno convenuto una dichiarazione[13] in cui si sottolinea la necessità di garantire la sicurezza dei dati per il grande pubblico e le imprese e di salvaguardare la sicurezza dell'ambiente digitale per tutti. Hanno inoltre concordato una serie di principi del G20 per un ambiente digitale sicuro e favorevole per i minori.

L'UE è stata una forte sostenitrice della cooperazione multilaterale, ritenendo che sia essenziale mantenere il ciberspazio aperto, stabile e sicuro. Nel novembre 2021, nel contesto del Forum di Parigi per la pace, la presidente von der Leyen ha annunciato la decisione di sostenere l'**appello di Parigi per la fiducia e la sicurezza nel ciberspazio**, unendosi agli oltre 80 Stati, 700 imprese e 350 organizzazioni della società civile che si impegnano a

[10] COM(2021) 7672 final.

[11] Dichiarazione dell'alto rappresentante a nome dell'Unione europea che esorta le autorità cinesi ad agire contro le attività informatiche dolose intraprese dal loro territorio, 19 luglio 2021.

[12] Dichiarazione dell'alto rappresentante a nome dell'Unione europea sul rispetto dei processi democratici dell'UE, 24 settembre 2021.

[13] https://www.g20.org/wp-content/uploads/2021/08/DECLARATION-OF-G20-DIGITAL-MINISTERS-2021_FINAL.pdf.

collaborare per affrontare le sfide poste dal ciberspazio ma anche le opportunità che esso offre.

L'UE si impegna inoltre a livello bilaterale con una serie di paesi terzi, anche attraverso dialoghi regolari in materia di sicurezza e ciberspazio. La cooperazione UE-USA sulle questioni di sicurezza ha acquisito slancio negli ultimi mesi ed è un esempio emblematico di collaborazione con paesi che condividono gli stessi principi per far progredire l'agenda in materia di sicurezza.

Cooperazione UE-USA in materia di sicurezza

Il vertice UE-USA del 15 giugno 2021 ha sottolineato la rinnovata determinazione ad affrontare congiuntamente le sfide comuni nel settore della sicurezza. Sono seguite diverse iniziative:

- il **Consiglio UE-USA per il commercio e la tecnologia** si è riunito una prima volta il 29 settembre 2021. La relativa dichiarazione di Pittsburgh[14] ha sottolineato l'importanza di controllare gli investimenti per affrontare i rischi per la sicurezza nazionale, di cooperare in settori connessi al controllo delle esportazioni per gli scambi di prodotti a duplice uso, di espandere le catene di approvvigionamento resilienti e sostenibili, nonché di affrontare la manipolazione delle informazioni e le ingerenze straniere. Il Consiglio UE-USA per il commercio e la tecnologia comprende un gruppo di lavoro dedicato alle **tecnologie dell'informazione e della comunicazione e ai servizi, alla sicurezza e alla competitività**, che si occuperanno di questioni quali la sicurezza, la diversità, l'interoperabilità e la resilienza lungo la catena di approvvigionamento delle TIC, tra cui ambiti critici e sensibili come il 5G, i cavi sottomarini, i centri dati e l'infrastruttura cloud; il 21 settembre 2021 si è tenuto un **dialogo UE-USA in materia di ciberspazio**. È stato raggiunto un accordo sulla necessità di intensificare la cooperazione e il coordinamento in merito alle discussioni delle Nazioni Unite in materia di ciberspazio, di prevenire, scoraggiare e affrontare le attività informatiche dolose e di impegnarsi efficacemente con altri paesi, in particolare per aumentare la resilienza a livello mondiale;
- nell'ottobre 2021 l'UE ha partecipato all'**iniziativa "Counter Ransomware"** della Casa Bianca[15], unitamente a esperti di alto livello e rappresentanti governativi di 30 paesi. Le discussioni hanno riguardato la resilienza della rete, l'uso improprio della valuta virtuale per riciclare i pagamenti dei riscatti, lo scambio di informazioni a sostegno delle indagini e dell'azione penale nei confronti degli autori di attacchi ransomware transnazionali e gli sforzi diplomatici per sostenere gli obiettivi condivisi di contrasto degli attacchi ransomware. Un **gruppo di lavoro UE-USA sugli attacchi ransomware** incentrato sulla cooperazione operativa tra le autorità di contrasto si è riunito per la prima volta il 25 ottobre 2021;
- a margine della riunione del G20 dell'ottobre 2021, l'UE ha discusso con gli Stati Uniti e altri partecipanti in merito alle **interruzioni a breve termine della catena di approvvigionamento** e ai percorsi verso la resilienza a lungo termine, al fine di evitare carenze e mantenere l'apertura dei mercati[16].

[14] Dichiarazione comune inaugurale del Consiglio UE-USA per il commercio e la tecnologia (europa.eu).
[15] Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting (ottobre 2021).
[16] Chair's Statement on Principles for Supply Chain Resilience, 31 ottobre 2021, Casa Bianca.

Al fine di contrastare efficacemente la **criminalità informatica**, si stanno compiendo sforzi in tutto il mondo, a livello nazionale, dell'UE[17] e internazionale, per migliorare l'accesso transfrontaliero alle prove elettroniche per le indagini penali. Norme compatibili a livello internazionale sono particolarmente importanti per evitare conflitti di leggi quando si cerca di ottenere l'accesso transfrontaliero alle prove elettroniche.

Importanti progressi su questo fronte sono stati compiuti con la conclusione formale dei negoziati sul secondo protocollo addizionale alla Convenzione sulla criminalità informatica (**Convenzione di Budapest**) nell'ambito del Consiglio d'Europa, con l'adozione del testo da parte del Comitato dei Ministri del Consiglio d'Europa il 17 novembre 2021. La Commissione ha adottato proposte per autorizzare gli Stati membri, nell'interesse dell'Unione, a firmare e ratificare rapidamente il protocollo[18] e sta ora lavorando a stretto contatto con il Parlamento europeo e il Consiglio per consentire agli Stati membri di procedere quanto prima alla firma e alla ratifica. Il protocollo fornisce agli operatori di tutto il mondo gli strumenti per rafforzare la cooperazione in materia di criminalità informatica e di prove elettroniche e riconosce che un'efficace cooperazione transfrontaliera a fini di giustizia penale beneficia di solide garanzie per la protezione dei diritti fondamentali. Il protocollo prevede anche garanzie per la tutela della vita privata e dei dati personali.

Parallelamente è in preparazione una nuova convenzione delle Nazioni Unite sulla criminalità informatica, che dovrebbe essere giuridicamente coerente con gli strumenti esistenti, in particolare la convenzione di Budapest. La Commissione garantirà l'effettiva partecipazione dell'Unione europea ai negoziati avviati nel gennaio 2022.

III. Affrontare le minacce in evoluzione

Le principali minacce in evoluzione osservate durante il periodo di riferimento riguardano le minacce **ibride** e l'evoluzione costante degli **sviluppi tecnologici**. La portata, la natura mutevole e il modus operandi delle minacce ibride e alla sicurezza rappresentano oggi una sfida costante e la varietà degli strumenti utilizzati dai malintenzionati è in espansione. Le sfide in materia di sicurezza derivano inoltre sempre più dall'evoluzione degli sviluppi tecnologici che, pur offrendo nuove opportunità alla società, sono spesso sfruttati anche da malintenzionati e criminali.

Al fine di affrontare efficacemente le minacce in evoluzione, la presidente von der Leyen[19] ha sottolineato la necessità di un approccio globale basato su una valutazione comune delle minacce. La **bussola strategica** presentata dall'alto rappresentante nel novembre 2021 e che dovrebbe essere approvata dagli Stati membri nel marzo 2022 costituirà un documento di orientamento per le politiche dell'UE in materia di sicurezza e difesa. Sulla base della prima analisi globale delle minacce condotta dall'UE nel 2020, la bussola strategica indica il percorso da seguire affinché l'UE rafforzi l'autonomia strategica e diventi un partner globale

[17] Il pacchetto relativo alle prove elettroniche (COM(2018) 225 final e COM(2018) 226 final), ancora in corso di negoziazione da parte del Parlamento europeo e del Consiglio, fornirebbe alle autorità giudiziarie e di contrasto nazionali dell'UE gli ordini europei di produzione e gli ordini europei di conservazione per ottenere in modo rapido dai prestatori di servizi prove digitali per le indagini penali, indipendentemente dal luogo in cui è stabilito il prestatore o sono conservate le informazioni, e al tempo stesso fornirebbe solide garanzie.

[18] COM(2021) 718 final e COM(2021) 719 final.

[19] Stato dell'Unione 2021, discorso della presidente Ursula von der Leyen, 15 settembre 2021.

più forte. Essa definisce obiettivi e risultati tangibili per i prossimi 5-10 anni riguardo a come agire rapidamente in caso di crisi, proteggere i nostri cittadini dalle minacce in rapida evoluzione, investire nelle capacità di cui abbiamo bisogno e collaborare con altri per raggiungere obiettivi comuni.

L'esperienza della pandemia di COVID-19 ha dimostrato che **la manipolazione delle informazioni e le ingerenze straniere** costituiscono una minaccia grave e crescente per la sicurezza. Esse possono mettere a repentaglio i valori sanciti dai trattati dell'UE, in particolare le istituzioni e i processi democratici, e compromettere i diritti e le libertà fondamentali. L'UE è attiva nel rilevare, analizzare e mettere in luce la manipolazione delle informazioni e le ingerenze straniere e collabora strettamente con i paesi terzi e i partner internazionali (in particolare il G7 e la NATO) per costruire le capacità. A seguito del piano d'azione per la democrazia europea[20], il servizio europeo per l'azione esterna sta elaborando, in stretta cooperazione con la Commissione europea, un insieme di strumenti per contrastare la manipolazione delle informazioni e le ingerenze straniere. Il 25 novembre la Commissione ha presentato una serie di iniziative volte a rafforzare la democrazia e l'integrità delle elezioni, tra cui una proposta di regolamento relativo alla trasparenza[21] della pubblicità politica e due proposte che aggiornano le direttive sui diritti elettorali dei "cittadini mobili dell'UE"[22].

Un importante sviluppo per quanto riguarda gli attacchi ibridi contro l'UE nell'estate del 2021 è stato un tentativo di destabilizzare l'UE attraverso la strumentalizzazione dei migranti alle frontiere esterne dell'UE.

L'attacco ibrido della Bielorussia contro l'UE

- Nell'estate del 2021 la Bielorussia è stata oggetto di sanzioni dopo l'atterraggio forzato di un aereo passeggeri nel maggio 2021. Il regime ha reagito agevolando gli arrivi di migranti irregolari alle frontiere di Lituania, Lettonia e Polonia, un'azione che dimostra il tentativo determinato di produrre una crisi prolungata nel quadro di un più ampio sforzo concertato volto a destabilizzare l'UE.
- Oltre all'esposizione dei migranti a un rischio personale significativo, una componente importante dell'azione della Bielorussia volta a strumentalizzare i migranti è stata la manipolazione delle informazioni. L'UE ha monitorato, analizzato e messo in luce la manipolazione delle informazioni e le ingerenze straniere e ha condiviso le sue conclusioni con gli Stati membri e i partner internazionali (NATO e G7) attraverso il sistema di allarme rapido.
- La comunicazione congiunta del 23 novembre "Risposta alla strumentalizzazione dei migranti avallata dallo Stato alle frontiere esterne dell'UE"[23], definisce la risposta solida e variegata dell'UE a questi eventi.

[20] COM(2020) 790 final.
[21] COM(2021) 731 final.
[22] COM(2021) 732 final e COM(2021) 733 final.
[23] JOIN(2021) 32 final.

- Questa comprende una serie di misure, tra cui: il sostegno finanziario dell'UE; l'assistenza operativa agli Stati membri colpiti da parte delle agenzie dell'UE **Frontex** ed **EASO**; attività diplomatiche di sensibilizzazione nei confronti dei paesi di origine e di transito per evitare che i loro cittadini cadano in trappola; l'adozione di sanzioni nei confronti di coloro che facilitano gli attraversamenti illegali alle frontiere esterne dell'Unione[24]. È stato proposto un progetto di regolamento per limitare le attività degli operatori dei trasporti che facilitano il traffico o la tratta di esseri umani verso l'UE[25]. Sono state proposte misure straordinarie in materia di asilo e rimpatrio per aiutare gli Stati membri colpiti a rispondere alla crisi attuale, nel pieno rispetto dei valori e delle norme dell'UE[26]. La proposta di revisione del codice frontiere Schengen integrerà a sua volta questo insieme di strumenti, definendo la strumentalizzazione nel quadro giuridico dell'UE.

Prosegue l'attuazione del quadro congiunto per contrastare le minacce ibride del 2016 e della comunicazione congiunta del 2018 "Rafforzamento della resilienza e potenziamento delle capacità per affrontare le minacce ibride", come descritto nella quinta relazione annuale[27]. Le considerazioni relative alle minacce ibride sono integrate nell'elaborazione delle politiche, nell'ambito della valutazione d'impatto delle prossime iniziative politiche dell'UE, nel quadro degli strumenti per legiferare meglio. È stata rafforzata la rete di punti di contatto, che ora comprende funzionari responsabili delle politiche provenienti da tutti i servizi della Commissione, dal servizio europeo per l'azione esterna e dall'Agenzia europea per la difesa.

Per contrastare le minacce ibride è anche fondamentale rafforzare la conoscenza situazionale e sviluppare la resilienza. La **cellula per l'analisi delle minacce ibride** presso il centro dell'UE di analisi dell'intelligence, che opera nell'ambito del servizio europeo per l'azione esterna, ha prodotto oltre 100 relazioni scritte sulle minacce ibride, tra cui sei analisi delle tendenze nel campo delle minacce ibride. Al fine di sviluppare strumenti per valutare il livello di preparazione nei settori esposti a ingerenze sotto forma di minacce ibride, i servizi della Commissione e il servizio europeo per l'azione esterna hanno effettuato una **prima individuazione di parametri di riferimento settoriali**, che rappresenta un primo passo nel monitoraggio dei progressi compiuti nella protezione degli Stati membri e delle istituzioni dell'UE dalle minacce ibride.

Le minacce ibride sono anche al centro della **cooperazione UE-NATO**, basata sulle dichiarazioni congiunte di Varsavia e Bruxelles del 2016 e del 2018, che si è ulteriormente intensificata durante la pandemia di COVID-19[28]. Alla luce della continua evoluzione delle minacce cui devono far fronte gli Stati membri dell'UE e gli alleati della NATO, sono in corso i negoziati per una terza dichiarazione congiunta UE-NATO.

[24] Decisione 2021/1990 del Consiglio che modifica la decisione 2012/642/PESC relativa a misure restrittive in considerazione della situazione in Bielorussia e regolamento (UE) 2021/1985 del Consiglio che modifica il regolamento (CE) n. 765/2006 concernente misure restrittive nei confronti della Bielorussia (GU L 405 del 16.11.2021, pag. 1 e pag. 10).

[25] COM(2021) 753 final.

[26] COM(2021) 752 final.

[27] SWD(2021) 729 final.

[28] Cfr. la sesta relazione sullo stato dei lavori relativi all'attuazione dell'insieme comune di proposte approvato dai Consigli dell'UE e della NATO il 6 dicembre 2016 e il 5 dicembre 2017, 3 giugno 2021.

Rischi chimici, biologici, radiologici e nucleari (CBRN)

Le minacce di origine biologica, chimica e ignota possono costituire minacce transfrontaliere per la salute ed essere utilizzate come minacce ibride o a fini terroristici. Tale aspetto sarà trattato nell'ambito del mandato dell'HERA attraverso continue valutazioni delle minacce e la promozione dell'approvvigionamento e della produzione di contromisure mediche pertinenti. L'UE inoltre finanzia (con 5 milioni di EUR dal programma in materia di salute) un'azione comune specificamente concepita per rafforzare la preparazione e la risposta agli attacchi terroristici biologici e chimici[29].

Sfide tecnologiche

Tecnologie quali la crittografia o l'intelligenza artificiale possono essere sfruttate da malintenzionati e criminali. In questo contesto, la sfida per i responsabili delle politiche in Europa e altrove consiste nel trovare il giusto equilibrio tra la tutela dei diritti e delle libertà individuali, la garanzia della cibersicurezza e la garanzia che le autorità di contrasto possano svolgere il loro lavoro.

Come sottolineato nella terza relazione sulla funzione di osservatorio in materia di crittografia[30], le autorità giudiziarie e di contrasto si trovano ad affrontare numerose sfide per intercettare legalmente le comunicazioni e raccogliere prove per le indagini penali. Nella strategia di quest'anno per la lotta alla criminalità organizzata, la Commissione ha espresso l'intenzione di suggerire un percorso da seguire nel 2022 per affrontare la questione dell'accesso legittimo e mirato alle **informazioni criptate** nell'ambito delle indagini e delle azioni penali. La Commissione sta svolgendo un esercizio di mappatura della legislazione, della giurisprudenza, delle prassi operative e delle esigenze esistenti negli Stati membri, al fine di acquisire una comprensione più approfondita dei quadri giuridici, delle prassi attuali e delle esigenze delle autorità di contrasto, del sistema giudiziario e delle comunità di cibersicurezza.

Le discussioni sulla proposta della Commissione relativa a una legge sull'**intelligenza artificiale** hanno avuto luogo in sede di Consiglio "Giustizia e affari interni" e "Telecomunicazioni". La presidenza slovena ha organizzato seminari, dedicati, tra l'altro, alle attività di contrasto, per chiarire le questioni più complesse. Nel giugno 2021 il comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (GEPD) hanno pubblicato un parere congiunto sulla proposta della Commissione[31], chiedendo un divieto generale di qualsiasi uso dell'IA per i sistemi di identificazione biometrica remota negli spazi pubblici. Il 6 ottobre 2021 il Parlamento europeo ha adottato una risoluzione[32] in cui richiama l'attenzione sul rischio di sistemi di identificazione biometrica remota in tempo reale e di distorsioni algoritmiche nelle applicazioni di IA e

---

[29] Il lavoro intrapreso dal consorzio JA TERROR si concentrerà specificamente sulla fornitura di conoscenze e informazioni a tutti i settori pertinenti per sostenere la preparazione sanitaria e rafforzare la risposta intersettoriale (salute, sicurezza e protezione civile) agli attacchi terroristici biologici o chimici. Il gruppo comprende portatori di interessi di 18 paesi europei, con 14 Stati membri, un membro del SEE, un paese candidato, un paese candidato potenziale e il Regno Unito. Visti gli obiettivi condivisi, l'HERA opererà anche in stretta collaborazione con questo consorzio.

[30] Terza relazione sulla funzione di osservatorio in materia di crittografia, 2 luglio 2021.

[31] EDPB-GEPD Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale).

[32] Risoluzione del Parlamento europeo, del 6 ottobre 2021, sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale.

sottolinea la necessità di una supervisione umana e di forti poteri giuridici, in particolare in contesti di attività di contrasto o di attraversamento delle frontiere.

IV. Proteggere gli europei dal terrorismo e dalla criminalità organizzata

Terrorismo

La relazione sulla situazione e sulle tendenze del terrorismo pubblicata da Europol nel giugno 2021[33] indicava che gli Stati membri ritenevano che il terrorismo jihadista rimanesse la principale minaccia terroristica nell'UE. La relazione conferma che il tipo più frequente di attacchi ispirati al jihadismo nell'UE, in Svizzera e nel Regno Unito sono state le aggressioni in luoghi pubblici nei confronti di civili. Tutti gli attacchi jihadisti portati a termine nel 2020 sono stati commessi da persone che agivano da sole. La relazione indica inoltre che diversi sospetti arrestati nel 2020 avevano contatti online con i seguaci di gruppi terroristici al di fuori dell'UE. L'autoproclamato gruppo terroristico dello Stato islamico e la rete Al-Qaeda hanno continuato a incitare ad attacchi solitari nei paesi occidentali[34], dimostrando come la sicurezza esterna e interna siano strettamente interconnesse. In agosto il Consiglio "Giustizia e affari interni" ha dichiarato che "l'UE e i suoi Stati membri faranno tutto il possibile per garantire che la situazione in Afghanistan non comporti nuove minacce alla sicurezza per i cittadini dell'UE"[35]. Sono state adottate misure per garantire che tutti gli strumenti disponibili siano utilizzati per rispondere a possibili minacce.

Alla luce degli sviluppi in Afghanistan, il coordinatore antiterrorismo dell'UE, in coordinamento con la Commissione, il servizio europeo per l'azione esterna, la presidenza e le principali agenzie dell'UE, ha elaborato **un piano d'azione antiterrorismo sull'Afghanistan**[36]. Il piano d'azione formula 23 raccomandazioni in quattro ambiti: verifiche di sicurezza — prevenire le infiltrazioni; impedire che l'Afghanistan diventi un rifugio sicuro per i gruppi terroristici; monitorare e contrastare la propaganda e la mobilitazione (ad esempio il ruolo della rete di sensibilizzazione al problema della radicalizzazione); e contrastare la criminalità organizzata quale fonte di finanziamento del terrorismo. Il piano d'azione è stato accolto con favore dagli Stati membri in occasione del Consiglio "Giustizia e affari interni" dell'8 ottobre 2021. Un primo risultato è stata una procedura volontaria per il rafforzamento delle verifiche di sicurezza sulle persone provenienti dall'Afghanistan, approvata dal comitato permanente dell'UE per la cooperazione operativa in materia di sicurezza interna il 22 novembre 2021. In una riunione tecnica tenutasi il 28 novembre 2021 a Doha con i membri del governo afghano provvisorio proclamato dai talebani[37], l'UE ha esortato l'Afghanistan ad adottare misure risolute per combattere tutte le forme di terrorismo.

La Commissione prosegue i lavori sull'attuazione del programma di lotta al terrorismo. **Una valutazione della direttiva sulla lotta contro il terrorismo**[38] è stata adottata il 18 novembre 2021[39] con un giudizio generalmente positivo. Vi sono tuttavia problemi che limitano le prestazioni, ad esempio difficoltà nel dimostrare l'intento terroristico o, in alcuni Stati

[33] Relazione di Europol sulle tendenze e la situazione del terrorismo nell'UE (Te-Sat), 22 giugno 2021.
[34] Relazione di Europol sulle tendenze e la situazione del terrorismo nell'UE (Te-Sat), 22 giugno 2021.
[35] Dichiarazione sulla situazione in Afghanistan, 11385/21, 31 agosto 2021.
[36] Afghanistan: piano d'azione per la lotta al terrorismo, 29 settembre 2021.
[37] Tale dialogo non implica il riconoscimento del governo provvisorio da parte dell'UE, ma rientra nell'impegno operativo dell'UE, nell'interesse dell'UE e del popolo afghano.
[38] Direttiva (UE) 2017/541, del 15 marzo 2017, sulla lotta contro il terrorismo (GU L 88 del 15.3.2017, pag. 6).
[39] COM(2021) 701 final.

membri, sfide relative alla classificazione come atti di terrorismo degli atti di estremismo violento di destra.

Permangono infine ostacoli all'efficacia della cooperazione e del coordinamento tra gli Stati membri per quanto riguarda **la protezione e l'assistenza alle vittime del terrorismo**. La Commissione sta valutando ulteriormente il recepimento della direttiva nel diritto nazionale e dal luglio 2021 ha avviato procedure di infrazione nei confronti di 24 Stati membri per non aver recepito adeguatamente la direttiva. Il progetto pilota del centro di competenza dell'UE per le vittime del terrorismo[40] ha aiutato gli Stati membri e le organizzazioni nazionali di sostegno alle vittime nell'applicazione pratica delle norme dell'UE relative alle vittime del terrorismo. I risultati di questo progetto pilota comprendono il manuale dell'UE sulle vittime del terrorismo, manuali nazionali e oltre 750 partecipanti ad attività di formazione nazionali.

La Commissione sostiene costantemente gli sforzi degli Stati membri volti a proteggere meglio gli spazi pubblici. È stata organizzata una seconda Autumn School digitale per la protezione degli spazi pubblici e i portatori di interessi sono aggiornati sulle migliori pratiche[41].

Per prevenire meglio il terrorismo, la lotta contro la radicalizzazione, sia offline che online, deve proseguire. Nell'ottobre 2021 la **rete di sensibilizzazione al problema della radicalizzazione (RAN)** ha celebrato il suo 10º anno di prevenzione della radicalizzazione con una conferenza incentrata sull'evoluzione delle sfide in questo settore. Per quanto riguarda la lotta contro la radicalizzazione online, il 5 novembre 2021 **Europol**, in cooperazione con la Commissione, ha organizzato un'esercitazione per testare l'attuazione del protocollo di crisi dell'UE[42]. L'esercitazione si è svolta nel quadro del Forum dell'UE su internet e ha esaminato la cooperazione tra le autorità governative e l'industria tecnologica per contenere la diffusione virale di contenuti terroristici ed estremisti violenti online.

Poiché la sicurezza dei nostri partner e dei nostri vicini è essenziale per garantire la sicurezza interna dell'Europa, il servizio europeo per l'azione esterna e la Commissione lavorano a stretto contatto con i principali paesi terzi e le organizzazioni internazionali attraverso regolari **dialoghi in materia di lotta al terrorismo** per rafforzare la nostra cooperazione sulle questioni relative alla sicurezza e alla lotta al terrorismo. Allo stesso tempo, sono stati conclusi vari accordi per facilitare lo scambio di informazioni e di dati personali, il che a sua volta consente una cooperazione più operativa tramite Europol.

Dialoghi in materia di lotta al terrorismo con paesi terzi/organizzazioni internazionali tra luglio e dicembre 2021

Dialogo ad alto livello in materia di politica e di sicurezza con l'Asia centrale (luglio 2021)

- Comitato misto di cooperazione con la Nuova Zelanda, dialogo strategico UE-Nuova Zelanda (luglio 2021)
- Riunione degli alti funzionari delle Maldive, sezione Lotta al terrorismo (settembre

[40] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/protecting-victims-rights/eu-centre-expertise-victims-terrorism_en.

[41] Cfr. la newsletter sulla protezione degli spazi pubblici: https://europa.eu/!jV87NK.

[42] Il protocollo di crisi dell'UE, adottato dai ministri della Giustizia e degli Interni nell'ottobre 2019, è un meccanismo volontario che consente agli Stati membri dell'UE e alle piattaforme online di rispondere rapidamente e in modo coordinato di diffusione di contenuti terroristici online nel caso di un attacco terroristico, garantendo nel contempo una forte protezione dei dati e la salvaguardia dei diritti fondamentali.

2021)
- Dialogo sulla lotta al terrorismo con la Bosnia-Erzegovina (ottobre 2021)
- Dialogo sulla lotta al terrorismo con la Turchia (25 novembre 2021)
- Dialogo UE-NATO sulla lotta al terrorismo (15 novembre 2021)

Accordi Europol con paesi terzi sullo scambio di dati personali

- Accordo Europol con la Nuova Zelanda concluso il 28 settembre 2021
- Il primo ciclo di negoziati con Israele si è svolto il 22 novembre 2021

Accordi di cooperazione strategica Europol

- Europol ha firmato un accordo di cooperazione strategica con l'Armenia il 16 settembre 2021

Con i Balcani occidentali esiste una cooperazione particolarmente intensa in materia di lotta al terrorismo e prevenzione della radicalizzazione, nel quadro del piano d'azione comune del 2018 per i Balcani occidentali sulla lotta al terrorismo[43]. I lavori per l'attuazione dei sei accordi di attuazione con ciascun partner dei Balcani occidentali proseguono a ritmo sostenuto. Il vertice UE-Balcani occidentali tenutosi in Slovenia nell'ottobre 2021 ha sottolineato l'importanza di adottare misure risolute per affrontare il terrorismo e la radicalizzazione, la criminalità organizzata e le forme gravi di criminalità, in particolare la tratta di esseri umani, il traffico di migranti, il riciclaggio di denaro, la coltivazione e il traffico di droga, nonché la corruzione, il traffico illecito di armi da fuoco e le minacce informatiche e ibride.

Il 20 luglio 2021 la Commissione ha presentato un ambizioso pacchetto di proposte legislative per rafforzare le **norme dell'UE in materia di antiriciclaggio e contrasto del finanziamento del terrorismo (AML/CFT)**[44], comprese misure relative alle cripto-attività per allinearsi alle più recenti norme internazionali elaborate dal Gruppo di azione finanziaria internazionale (GAFI). Ad esempio, tutti i fornitori di servizi per le cripto-attività saranno inclusi nell'ambito di applicazione della legislazione antiriciclaggio dell'UE, che impone loro di segnalare eventuali operazioni sospette effettuate dai clienti. La Commissione propone inoltre di vietare la fornitura di portafogli di cripto-attività anonimi da parte dei fornitori di servizi per le cripto-attività. Il pacchetto fa parte dell'impegno della Commissione di proteggere le persone nell'UE e nel sistema finanziario dell'UE dal finanziamento del terrorismo. L'obiettivo è migliorare l'individuazione delle operazioni e delle attività sospette e colmare le lacune sfruttate dai criminali per riciclare proventi illeciti o finanziare attività terroristiche attraverso il sistema finanziario.

I nuovi recenti regolamenti sui controlli doganali sul denaro contante in entrata nell'Unione e in uscita dall'Unione[45] e sull'importazione di beni culturali[46] sono attualmente in fase di

[43] Nell'ottobre 2018 la Commissione e i rappresentanti di Albania, Bosnia-Erzegovina, Kosovo*, Montenegro, Macedonia del Nord e Serbia hanno firmato un piano d'azione comune per i Balcani occidentali sulla lotta al terrorismo.

[44] COM(2021) 421 final, COM(2021) 420 final, COM(2021) 423 final e COM(2021) 422 final.

[45] Regolamento (UE) 2018/1672 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, relativo ai controlli sul denaro contante in entrata nell'Unione o in uscita dall'Unione (GU L 284 del 12.11.2018, pag. 6).

attuazione[47] (attuazione parziale per il regolamento sull'importazione di beni culturali, in attesa dello sviluppo del relativo sistema informatico centralizzato). Tali regolamenti contribuiranno alla lotta contro il riciclaggio di denaro e alla protezione del patrimonio culturale, ma svolgeranno anche un ruolo nel rafforzare la lotta contro il finanziamento del terrorismo.

Criminalità organizzata

Le tendenze in materia di criminalità osservate da Europol durante la pandemia di COVID-19 mostrano che, nonostante i lockdown e le restrizioni, la criminalità organizzata e le forme gravi di criminalità rimangono attive, si adattano e sfruttano tutte le circostanze per realizzare un profitto. Mentre le economie legali si sono indebolite, l'economia criminale si è rafforzata. La cooperazione internazionale nell'attività di contrasto mostra quotidianamente la dimensione globale delle reti della criminalità organizzata e il grado di connettività tra i criminali. Per rispondere a questa sfida internazionale è necessario un impegno internazionale nella lotta alla criminalità organizzata, incluse ulteriori misure per sviluppare partenariati e cooperazione con i paesi nelle immediate vicinanze e oltre.

Il commercio di **droghe illecite** resta il più grande mercato criminale dell'UE. Il piano d'azione dell'UE in materia di droghe per il periodo 2021-2025 è stato adottato all'inizio di luglio, a seguito della pubblicazione della strategia nel dicembre 2020. I coordinatori nazionali antidroga dell'UE si sono riuniti il 22 settembre per discutere di prevenzione. In giugno l'**Osservatorio europeo delle droghe e delle tossicodipendenze** (EMCDDA) ha presentato la sua ultima analisi della situazione della droga in Europa nella relazione europea sulla droga del 2021[48] e in settembre ha pubblicato una relazione in cui sottolinea la crescente produzione di metamfetamina in Afghanistan[49]. **Europol** sta intensificando la cooperazione con le autorità iraniane e turche per migliorare le informazioni sul traffico di droga. Secondo Europol, la principale rotta del traffico di eroina all'interno dell'UE è ancora attraverso i Balcani, mentre il traffico di cocaina avviene più comunemente attraverso porti container come Anversa o Rotterdam. Europol sta realizzando una nuova piattaforma sulle droghe per aggiornare settimanalmente gli Stati membri dell'UE sugli sviluppi.

La cooperazione con i partner internazionali è fondamentale nella lotta contro la droga. I recenti contatti hanno incluso un dialogo UE-USA nel settembre 2021, il dialogo UE-Balcani occidentali in materia di droghe in ottobre e il meccanismo di coordinamento e cooperazione in materia di droghe UE-CELAC a giugno. Occorre istituire un dialogo UE-Iran e un dialogo UE-Colombia in materia di droghe.

---

[46] Regolamento (UE) 2019/880 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'introduzione e all'importazione di beni culturali (GU L 151 del 7.6.2019, pag. 1).

[47] Regolamento di esecuzione 2021/1079 della Commissione ai fini del regolamento (UE) 2019/880 del Parlamento europeo e del Consiglio relativo all'introduzione e all'importazione di beni culturali (adottato dalla Commissione il 24.6.2021) e decisione di esecuzione della Commissione relativa ai criteri per il quadro comune di gestione del rischio sui movimenti di contante ai fini del regolamento (UE) 2018/1672 del Parlamento europeo e del Consiglio relativo ai controlli sul denaro contante in entrata nell'Unione o in uscita dall'Unione (adozione prevista per dicembre 2021).

[48] https://www.emcdda.europa.eu/publications/edr/trends-developments/2021_en.

[49] https://www.emcdda.europa.eu/publications/ad-hoc-publication/methamphetamine-from-afghanistan-signals-indicate-europe-should-be-better-prepared_en.

Il piano d'azione 2020-2025 dell'UE sul **traffico di armi da fuoco**[50] chiarisce che la piena attuazione della direttiva sulle armi da fuoco è una priorità assoluta. La relazione della Commissione dell'ottobre 2021 valuta l'applicazione della direttiva relativa al controllo dell'acquisizione e della detenzione di armi[51], rilevando che la direttiva sulle armi da fuoco ha migliorato le categorie di armi da fuoco, la loro tracciabilità, gli scambi di informazioni e le procedure amministrative. Tuttavia finora solo dieci Stati membri hanno pienamente recepito la direttiva. La relazione sottolinea che è possibile compiere ulteriori progressi nel controllo giuridico dell'acquisizione, della detenzione e della circolazione delle armi civili. La Commissione effettuerà pertanto una valutazione d'impatto sulla possibile modifica alla direttiva sulle armi da fuoco. Vi sono circa 35 milioni di armi da fuoco illegali nell'UE e molte di esse sono contrabbandate attraverso le nostre frontiere. La cooperazione con i Balcani occidentali è fondamentale. Nel settembre 2021 si è tenuta una conferenza ministeriale UE-Balcani occidentali sulle armi da fuoco, che ha sottolineato la stretta cooperazione tra l'UE e i Balcani occidentali contro il traffico di armi da fuoco nell'ambito della piattaforma multidisciplinare europea di lotta alle minacce della criminalità (**EMPACT**). Dall'adozione della tabella di marcia regionale per tutte le armi leggere e di piccolo calibro nel 2018, i partner dei Balcani occidentali hanno compiuto costanti progressi nell'armonizzazione dei quadri giuridici con le norme dell'UE e delle Nazioni Unite in materia di armi da fuoco e si è registrato un aumento della cooperazione operativa e dello scambio di informazioni con l'UE e le sue agenzie.

Il **traffico di rifiuti**[52] è una delle forme più gravi di criminalità ambientale. Fino al 30 % delle spedizioni di rifiuti, per un valore annuo pari a 9,5 miliardi di EUR, è illegale. Il 17 novembre 2021 la Commissione ha adottato il regolamento riveduto sulle spedizioni di rifiuti, che rafforzerà ulteriormente l'azione contro il traffico di rifiuti istituendo un gruppo UE di garanzia della legalità delle spedizioni di rifiuti, conferendo all'Ufficio europeo per la lotta antifrode OLAF il potere di sostenere le indagini transnazionali condotte dagli Stati membri sul traffico di rifiuti e prevedendo norme più severe in materia di sanzioni amministrative.

La **lotta contro la corruzione** è fondamentale per garantire uno Stato di diritto forte e preservare la fiducia dei cittadini nelle istituzioni pubbliche. Il forte legame tra criminalità organizzata e corruzione, nonché il rischio di infiltrazioni nell'economia lecita e nelle istituzioni pubbliche sono sfide fondamentali. La seconda relazione sullo Stato di diritto pubblicata il 20 luglio 2021[53] ha evidenziato che, sebbene gli Stati membri dell'UE continuino a conseguire i risultati migliori a livello mondiale nella lotta contro la corruzione, permangono sfide, in particolare per quanto riguarda le indagini e le azioni penali e l'applicazione di sanzioni per corruzione in alcuni Stati membri. Sebbene molti Stati membri abbiano adottato misure volte a rafforzare i quadri per la prevenzione della corruzione e l'integrità, comprese le norme in materia di conflitti di interessi, trasparenza delle attività di lobbying e "porte girevoli", in alcuni Stati membri le risorse destinate alla lotta alla corruzione sono insufficienti. In altri persistono preoccupazioni circa l'efficacia delle indagini, delle azioni penali e delle sentenze relative ai casi di corruzione ad alto livello.

[50] COM(2020) 608 final.
[51] COM(2021) 647 final.
[52] COM(2021) 709 final.
[53] COM(2021) 700 final.

È inoltre essenziale prevenire le **frodi a danno del bilancio dell'UE**. Il 26 ottobre il Parlamento europeo ha pubblicato due relazioni[54], rilevando con preoccupazione che la pandemia di COVID-19 ha creato nuove opportunità per gli autori di frodi e la criminalità organizzata e richiamando l'attenzione sull'importanza delle misure preventive per anticipare e affrontare i rischi di corruzione in situazioni di crisi, nonché sulla necessità di una maggiore trasparenza nel contesto finanziario dell'Unione. Nel settembre 2021, a meno di quattro mesi dall'inizio delle sue attività, la Procura europea (EPPO) ha già conseguito notevoli risultati, avviando indagini su casi di presunta frode per un totale stimato di circa 4,5 miliardi di EUR[55]. Il 15 ottobre 2021 Europol ha istituito l'operazione Sentinel, una nuova operazione a livello dell'UE volta a contrastare le frodi a danno dei fondi offerti nel quadro dell'iniziativa NextGenerationEU, che coinvolge l'EPPO, Eurojust, l'OLAF e 23 Stati membri. Le attività dureranno almeno un anno e si concentreranno sullo scambio e la condivisione proattiva di informazioni e sul sostegno al coordinamento delle operazioni volte a contrastare le frodi a danno, in particolare, del dispositivo per la ripresa e la resilienza.

Il **traffico di migranti** è un'attività criminale che mira ad approfittare delle persone vulnerabili. Il 50 % dei trafficanti di esseri umani è costituito da policriminali impegnati in altre forme di attività criminale. Prevenire e combattere il traffico di migranti è un obiettivo fondamentale della strategia dell'UE per l'Unione della sicurezza, della strategia dell'UE per la lotta alla criminalità organizzata, della strategia dell'UE per la lotta alla tratta degli esseri umani (2021-2025) e del nuovo patto sulla migrazione e l'asilo, che richiede una cooperazione e un coordinamento internazionali costanti. Sulla base dei progressi compiuti dal primo piano d'azione dell'UE contro il traffico di migranti (2015-2020), la Commissione, in collaborazione con l'alto rappresentante, ha adottato un nuovo piano d'azione dell'UE per il periodo 2021-2025[56].

Temi chiave del piano d'azione dell'UE contro il traffico di migranti (2021-2025)

- Sviluppare **partenariati operativi per la lotta contro il traffico di migranti** con strumenti concreti nell'ambito di partenariati globali, equilibrati, su misura e reciprocamente vantaggiosi in materia di migrazione, consolidando ulteriormente la fiducia e la cooperazione reciproca.
- Migliorare l'attuazione dei quadri giuridici per il sanzionamento dei trafficanti e la protezione dallo sfruttamento.
- Rafforzare la cooperazione giudiziaria in materia di traffico di migranti invitando gli Stati membri dell'UE ad avvalersi maggiormente di **Eurojust**, a sostenere le indagini transfrontaliere attraverso squadre investigative comuni e fare il miglior uso possibile del gruppo di riflessione per procuratori contro il traffico di migranti.

[54] Relazione sulla valutazione delle misure preventive per evitare la corruzione, la spesa irregolare e l'uso improprio dei fondi UE e nazionali in caso di fondi di emergenza e settori di spesa connessi alle crisi (2020/2222 (INI)) e relazione sull'impatto della criminalità organizzata sulle risorse proprie dell'UE e sull'uso improprio dei fondi dell'UE con particolare attenzione alla gestione concorrente (2020/2221 (INI)).

[55] "Danni stimati al bilancio dell'UE nelle indagini in corso dell'EPPO: quasi 4,5 miliardi di EUR", disponibile all'indirizzo https://www.eppo.europa.eu/en/news/estimated-damages-eu-budget-ongoing-eppo-investigations-almost-eu45-billion.

[56] COM(2021) 591 final.

- Rispondere all'**evoluzione delle pratiche online** nonché degli strumenti che facilitano il traffico, rafforzando la cooperazione operativa e lo scambio di informazioni tra le autorità nazionali e le agenzie dell'UE.
- Aumentare **la ricerca e la raccolta di dati** per una migliore comprensione delle tendenze migratorie, della natura e della portata delle reti criminali, delle ripercussioni delle politiche antitraffico e del modus operandi delle reti criminali.

Il 4 e il 5 novembre 2021 **Eurojust** ha tenuto la sua riunione annuale sul traffico di migranti, che ha anche fornito l'opportunità di rafforzare la cooperazione in materia con i Balcani occidentali e i paesi partner meridionali del bacino del Mediterraneo che partecipano a EuroMed Justice. Negli ultimi sei mesi del 2021 Eurojust ha inoltre sostenuto diverse operazioni su larga scala contro il traffico di migranti[57].

A seguito della **strategia per la lotta alla tratta degli esseri umani**[58], la Commissione sta effettuando una valutazione della direttiva anti-tratta[59] che include una considerazione delle norme minime dell'UE che potrebbero configurare come reato l'uso di servizi derivanti dallo sfruttamento delle vittime della tratta. La XV Giornata europea contro la tratta di esseri umani si è svolta il 18 ottobre 2021 per sensibilizzare in merito a questo reato. Lo stesso giorno la rete delle agenzie GAI ha pubblicato una relazione congiunta[60] sull'identificazione e la protezione delle vittime della tratta di esseri umani. Nel novembre 2021 **Europol** e **Frontex** hanno coordinato un'azione internazionale su vasta scala contro la tratta di esseri umani. 29 paesi, guidati da Austria e Romania, hanno partecipato alle giornate di azione in cui oltre 14 000 funzionari delle autorità di contrasto sono intervenuti sulle rotte della tratta sulle strade e negli aeroporti, effettuando 212 arresti e individuando altre 89 persone sospettate di tratta.

L'**abuso sessuale dei minori** online e offline è uno dei reati più gravi e una priorità costante per l'UE e i suoi Stati membri. Il 12 novembre 2021 i ministri degli Interni hanno discusso politiche e pratiche volte a sensibilizzare in merito a questo reato e a prevenirlo, gli strumenti necessari per il buon esito delle indagini su questo reato, nel pieno rispetto dei diritti fondamentali di tutti gli utenti interessati, e le modalità per garantire la protezione delle vittime, con particolare attenzione ai diritti dei minori. La legislazione temporanea volta a garantire che i prestatori di servizi online possano continuare le loro pratiche volontarie per individuare e denunciare gli abusi sessuali sui minori online[61] e rimuovere il materiale pedopornografico dai loro sistemi è entrata in vigore il 3 agosto 2021. La Commissione continua a portare avanti i lavori sull'attuazione delle iniziative annunciate nella strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori e nella strategia globale dell'UE sui diritti dei minori e sta inoltre elaborando una legislazione a più lungo termine per combattere più efficacemente gli abusi sessuali sui minori online.

---

57 Cfr. ad esempio il link al comunicato stampa: https://www.eurojust.europa.eu/people-smuggling-network-netherlands-and-hungary-dismantled.

58 COM(2021) 171 final.

59 Direttiva 2011/36/UE del Parlamento europeo e del Consiglio, del 5 aprile 2011, concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime (GU L 101 del 15.4.2011, pag. 1).

60 Relazione congiunta della rete delle agenzie GAI sull'identificazione e la protezione delle vittime della tratta di esseri umani | Eurojust | Agenzia dell'Unione europea per la cooperazione giudiziaria penale (europa.eu).

61 COM(2020) 568 final.

V. Un forte ecosistema europeo della sicurezza

Il rafforzamento della cooperazione di polizia in tutta l'UE, nonché la solidità delle frontiere esterne, sono elementi essenziali di un'UE senza controlli alle frontiere interne. Data la natura transfrontaliera della lotta alla criminalità e del rafforzamento della sicurezza, gli Stati membri devono fare sempre più affidamento gli uni sugli altri. Permangono tuttavia ostacoli allo scambio di dati tra le autorità di contrasto di diversi Stati membri dell'UE, dai quali derivano punti ciechi che possono essere sfruttati da criminali e terroristi che agiscono in più di uno Stato membro[62]. Per sostenere meglio gli Stati membri, la Commissione presenta un pacchetto di misure sulla cooperazione di polizia.

Il **pacchetto sulla cooperazione di polizia** comprende:

- **proposta di direttiva sullo scambio di informazioni tra le autorità di contrasto degli Stati membri**[63]: gli obiettivi sono i) agevolare l'accesso equivalente delle autorità di contrasto alle informazioni disponibili in un altro Stato membro; ii) garantire che tutti gli Stati membri dispongano di un punto di contatto unico funzionante in modo efficace; iii) istituire l'applicazione di rete per lo scambio sicuro di informazioni di Europol (SIENA) come canale di comunicazione predefinito per lo scambio di informazioni tra Stati membri in materia di attività di contrasto;
- **proposta di raccomandazione del Consiglio sulla cooperazione operativa di polizia**[64]: gli obiettivi sono rafforzare la cooperazione operativa transfrontaliera tra forze di polizia mediante l'adozione di norme minime comuni dell'UE per gli strumenti di cooperazione in settori quali inseguimenti transfrontalieri, pattugliamenti congiunti e operazioni congiunte;
- **proposta di regolamento su Prüm II**[65]: l'obiettivo è rivedere l'attuale quadro di Prüm sullo scambio automatizzato di dati, anche i) aggiungendo le categorie dei precedenti penali e delle immagini facciali, ii) fornendo una soluzione tecnica (un router centrale) per un più efficiente scambio automatizzato di dati tra le autorità di contrasto e iii) garantendo che i dati pertinenti provenienti dalla banca dati di Europol siano messi a disposizione delle autorità di contrasto degli Stati membri.

Europol è fondamentale per la cooperazione di polizia contro il terrorismo e la criminalità organizzata. Un rapido accordo sulla proposta di modifica del regolamento Europol[66] consentirebbe a quest'ultimo di sostenere meglio gli Stati membri nella lotta contro la criminalità organizzata e il terrorismo.

La cooperazione a livello internazionale tra le autorità di contrasto è fondamentale per la nostra sicurezza interna. In luglio il Consiglio ha adottato un mandato negoziale per un accordo tra l'UE e **Interpol**. I negoziati dovrebbero iniziare nel dicembre 2021.

Per sostenere ulteriormente le indagini degli Stati membri sulla lotta al terrorismo e alla criminalità organizzata e agevolare la cooperazione giudiziaria, il 1º dicembre 2021 la Commissione ha adottato un **pacchetto sulla giustizia digitale**.

---

[62] Secondo la relazione SOCTA di Europol del 2021, oltre il 70 % dei gruppi della criminalità organizzata è presente in più di tre Stati membri.

[63] COM(2021) 782 final.

[64] COM(2021) 780 final.

[65] COM(2021) 784 final.

[66] COM(2020) 796 final.

Il **pacchetto sulla giustizia digitale** comprende:

- **proposta sullo scambio digitale di informazioni nei casi di terrorismo transfrontalieri**[67]: l'obiettivo è migliorare il funzionamento del registro antiterrorismo istituito nell'ottobre 2019. Ciò consentirà a **Eurojust** di svolgere un ruolo più incisivo e proattivo nel sostenere il coordinamento e la cooperazione tra le autorità nazionali responsabili delle indagini e dell'azione penale in relazione ai reati di terrorismo;
- **proposta sull'istituzione di una piattaforma di cooperazione come ausilio al funzionamento delle squadre investigative comuni**[68]: l'obiettivo è aumentare ulteriormente l'efficienza e l'efficacia delle squadre investigative comuni. Ciò consentirà la comunicazione elettronica e lo scambio di informazioni e prove in sicurezza tra le autorità nazionali competenti nonché gli organi, gli uffici e le agenzie dell'Unione coinvolti nelle rispettive squadre investigative comuni;
- **proposta sulla digitalizzazione della cooperazione giudiziaria transfrontaliera e sull'accesso alla giustizia in materia civile, commerciale e penale**[69]: la proposta mira a garantire un accesso effettivo alla giustizia per le persone fisiche e giuridiche e a facilitare la cooperazione giudiziaria tra gli Stati membri, fornendo una base giuridica per l'uso delle moderne tecnologie digitali per la comunicazione nel contesto dei procedimenti giudiziari transfrontalieri in materia civile, commerciale e penale.

Migliori sinergie tra sicurezza e difesa rafforzeranno l'efficacia della nostra azione a sostegno degli Stati membri in questi settori. La Commissione ha avviato l'attuazione del piano d'azione sulle **sinergie tra l'industria civile, della difesa e dello spazio**[70] adottato nel febbraio 2021**.** Essa collabora con le agenzie dell'UE, tra cui in particolare l'Agenzia europea per la difesa, per promuovere approcci basati sulle capacità in tutti i settori della sicurezza e per promuovere le sinergie attraverso un migliore coordinamento dei programmi e degli strumenti dell'UE. Inoltre la Commissione sta pubblicando un documento di lavoro dal titolo "Rafforzare la sicurezza attraverso la ricerca e l'innovazione". Tale documento, da un lato, sottolinea il ruolo strategico della ricerca in materia di sicurezza nel sostenere il conseguimento dei diversi obiettivi della politica di sicurezza civile e, dall'altro, illustra le misure in atto per consentire una diffusione ottimale dell'innovazione derivante dalla ricerca negli strumenti e nei servizi a disposizione delle autorità di sicurezza europee e nazionali.

Per quanto riguarda i finanziamenti dell'UE per la sicurezza, il programma di lavoro del Fondo sicurezza interna per il periodo 2021-2022 è stato adottato il 26 novembre 2021. Questo contribuirà ad azioni in una serie di settori quali lo scambio di informazioni, la cooperazione transfrontaliera, la prevenzione e il contrasto della criminalità organizzata, del terrorismo e della radicalizzazione offline e online. Il 10 novembre 2021 la Commissione ha adottato programmi di lavoro per il programma Europa digitale. Tra questi, il programma di lavoro sulla cibersicurezza, con un finanziamento pari a 269 milioni di EUR, sarà attuato dalla Commissione per conto del Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca (ECCC) insieme alla rete dei centri nazionali di coordinamento[71]. Tale programma vedrà investimenti nello sviluppo di

[67] COM(2021) 757 final.
[68] COM(2021) 756 final.
[69] COM(2021) 759 final.
[70] COM(2021) 70 final.
[71] Fino a quando l'ECCC non sarà in grado di eseguire il proprio bilancio, la Commissione europea attuerà le azioni nell'ambito di questo programma di lavoro in regime di gestione diretta per conto dell'ECCC.

attrezzature, strumenti e infrastrutture di dati avanzati per la cibersicurezza. Finanzierà lo sviluppo e l'uso ottimale della conoscenza e delle competenze relative alla cibersicurezza, promuoverà le migliori pratiche e garantirà un'ampia diffusione di soluzioni di cibersicurezza all'avanguardia nell'economia europea.

Un'attuazione rapida e completa della legislazione adottata è fondamentale per l'efficacia dell'Unione della sicurezza. Nelle sue decisioni sui casi di infrazione, la Commissione europea avvia un'azione legale nei confronti degli Stati membri che non rispettano i loro obblighi ai sensi del diritto dell'UE, compresa la legislazione nell'ambito dell'Unione della sicurezza. Il 2 dicembre la Commissione ha deciso di avviare procedimenti[72] contro vari Stati membri per non aver recepito o attuato determinati elementi delle norme dell'UE in materia di lotta al terrorismo, lotta contro il razzismo e la xenofobia, mandato d'arresto europeo, scambio di informazioni sui casellari giudiziali e lotta contro le frodi che ledono gli interessi finanziari dell'Unione mediante il diritto penale.

Il ruolo delle agenzie e degli organismi dell'UE

Le agenzie e gli organismi dell'UE hanno continuato a svolgere un ruolo cruciale nel promuovere la cooperazione e lo scambio di informazioni in tutta l'Unione e nel combattere la criminalità. Durante il periodo di riferimento molte delle loro attività si sono concentrate sulla risposta tempestiva alle esigenze operative derivanti dalla crisi afghana, ma anche su altre sfide urgenti in materia di sicurezza, quali minacce ibride, attacchi ransomware e criminalità organizzata.

Esempi di attività operative svolte dalle agenzie dell'UE

- Nell'ottobre 2021 le attività di cooperazione coordinate da **Europol** ed **Eurojust** hanno svolto un ruolo centrale nel contrastare gli attacchi ransomware alle infrastrutture critiche e nell'individuare una serie di responsabili delle minacce che hanno colpito oltre 1 800 vittime in 71 paesi[73].
- Nel luglio 2021 **Europol** ha celebrato il quinto anniversario dell'iniziativa "No More Ransom", che ha aiutato più di sei milioni di imprese e privati a recuperare gratuitamente i propri fascicoli, impedendo il pagamento di quasi un miliardo di euro ai criminali informatici.
- Il ruolo dell'**ENISA** nel settore della cooperazione operativa è stato consolidato con l'obiettivo di consentire alla rete di CSIRT[74], a CyCLONe[75] e a tutti gli attori coinvolti nell'UE di collaborare e reagire agli attacchi su vasta scala. Coordinando i segretariati sia di EU-CyCLONe sia della rete di CSIRT, l'ENISA mira a sincronizzare i livelli tecnico e operativo e tutti gli attori dell'UE coinvolti nella risposta.

Anche la cooperazione tra agenzie svolge un ruolo importante: ad esempio con l'accordo concluso il 22 novembre tra **Frontex** e l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (**eu-LISA**).

[72] https://ec.europa.eu/commission/presscorner/detail/it/INF_21_6201.

[73] https://www.eurojust.europa.eu/12-targeted-involvement-ransomware-attacks-against-critical-infrastructure.

[74] La rete di CSIRT è una rete composta dai gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) designati dagli Stati membri dell'UE e dalla squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'UE (CERT-UE).

[75] La rete delle organizzazioni di collegamento per le crisi informatiche.

La maggior parte delle agenzie sta sviluppando una dimensione esterna delle proprie attività. La cooperazione internazionale e questa dimensione esterna sono fondamentali per affrontare le sfide in materia di sicurezza su cui le agenzie sono incaricate di concentrarsi. L'attuazione di questa dimensione esterna avviene in stretta consultazione e coordinamento con altri attori e programmi esterni, compresa l'azione in materia di politica di sicurezza e di difesa comune (PSDC), al fine di evitare duplicazioni, consentire la cooperazione e migliorare l'efficacia.

Ruolo delle agenzie dell'UE nella risposta alla situazione in Afghanistan e nella regione

- Le agenzie dell'UE assicurano un monitoraggio costante della situazione in Afghanistan e nella regione e contribuiscono alla conoscenza situazionale e a uno scambio dinamico di informazioni sull'Afghanistan nel contesto della rete dell'UE per la preparazione e per la gestione delle crisi nel settore della migrazione (rete del programma).
- Il 31 agosto l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (**Europol**) ha pubblicato una relazione sul potenziale impatto degli sviluppi in Afghanistan che incidono sulla sicurezza interna dell'UE nei settori del terrorismo, della criminalità organizzata e del traffico di migranti. Europol ha inoltre avviato un gruppo di lavoro interno di esperti per monitorare la crisi e condividere informazioni pertinenti e affidabili.
- L'Ufficio europeo di sostegno per l'asilo (**EASO**) ha pubblicato una relazione informativa aggiornata sui paesi d'origine in merito alla situazione della sicurezza in Afghanistan e ha avviato attività di sostegno riguardanti sia la dimensione interna che quella esterna della crisi.
- L'Agenzia europea della guardia di frontiera e costiera (**Frontex**) ha monitorato la situazione e coordinato le operazioni congiunte degli Stati membri con i paesi terzi al fine di rafforzare la sicurezza delle frontiere, la cooperazione operativa e lo scambio di informazioni.

Dall'ultima relazione sui progressi compiuti nell'Unione della sicurezza, le agenzie e gli organismi dell'UE, oltre alle azioni operative descritte nella relazione, hanno pubblicato numerose relazioni e orientamenti preziosi che sono elencati nell'allegato.

VI. Conclusioni

L'UE continua a dimostrare di essere in grado di adattarsi e far fronte alle nuove sfide man mano che emergono, e ciò è particolarmente evidente nel settore della sicurezza. Che sia sostenendo gli Stati membri nell'affrontare le nuove minacce ibride alle frontiere esterne dell'UE o collaborando con partner internazionali per presentare una risposta coordinata alle minacce in continua evoluzione derivanti dalle nuove tecnologie, l'UE è costantemente aggiornata per proteggere i suoi Stati membri. Nel contempo i rischi più convenzionali per la sicurezza continuano a essere affrontati con soluzioni e azioni preventive a livello dell'UE.

Garantire la sicurezza dell'Europa nel suo insieme è una responsabilità comune, in cui ogni attore deve fare la propria parte, che sia mediante l'adozione di nuove norme efficaci e adeguate allo scopo da parte del Parlamento europeo e del Consiglio, l'attuazione tempestiva della legislazione dell'UE da parte degli Stati membri o il lavoro operativo svolto sul campo da varie autorità, organizzazioni e portatori di interessi. L'Unione della sicurezza continuerà a coordinare un'ampia gamma di strumenti e attori nell'interesse dei cittadini dell'UE.