Consiglio dell'Unione europea

Bruxelles, 16 dicembre 2022
(OR. en)

16124/22

JAI 1695	**DROIPEN 165**
COSI 328	**COPEN 450**
ENFOPOL 648	**FREMP 275**
ENFOCUSTOM 179	**JAIEX 106**
IXIM 298	**CFSP/PESC 1733**
CT 227	**COPS 616**
CRIMORG 184	**HYBRID 120**
FRONT 464	**DISINFO 112**
ASIM 108	**TELECOM 528**
VISA 203	**DIGIT 248**
CYBER 409	**COMPET 1045**
DATAPROTECT 369	**RECH 665**
CATS 74	**CULT 133**

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	13 dicembre 2022
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2022) 745 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO Quinta 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(2022) 745 final.

All.: COM(2022) 745 final

COMMISSIONE
EUROPEA

Bruxelles, 13.12.2022
COM(2022) 745 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

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

1. INTRODUZIONE

A luglio 2020 la Commissione ha adottato la strategia globale per l'Unione della sicurezza[1]. Da allora il contesto delle minacce è notevolmente mutato. La crisi dovuta alla COVID-19 ha accentuato alcune vulnerabilità, soprattutto a causa dell'incremento dell'attività online. Gli attacchi informatici hanno continuato ad aumentare in termini di portata e si sono diffuse in forme nuove[2]. La guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina ha avuto un impatto sulla sicurezza interna dell'UE, con l'aumento del rischio di tratta di esseri umani, la minaccia di incidenti chimici e nucleari e la circolazione illecita di armi da fuoco, e ha stimolato la manipolazione delle informazioni e l'ingerenza da parte di soggetti stranieri. Il recente sabotaggio dei gasdotti Nord Stream ha evidenziato come settori essenziali quali l'energia, le infrastrutture digitali, i trasporti e lo spazio dipendano dalla resilienza delle infrastrutture critiche, dimostrando ancora una volta come la sicurezza fisica e quella digitale siano strettamente interconnesse e debbano essere protette in parallelo.

La presente relazione sui progressi compiuti nella strategia dell'UE per l'Unione della sicurezza mira a fornire una panoramica "a medio termine" dell'attuazione della strategia, evidenziando ciò che è stato realizzato e ciò che rimane da fare entro la fine del mandato della Commissione. Da luglio 2020 l'UE ha compiuto grandi passi in avanti verso il completamento delle azioni nei settori chiave contemplati dai quattro pilastri della strategia[3]. La presente relazione mostra che la stragrande maggioranza delle azioni previste dalla strategia è stata attuata[4]. Resta tuttavia ancora molto da fare per sfruttare appieno l'impatto della strategia per l'Unione a vantaggio dei cittadini, in particolare l'adozione delle proposte legislative in sospeso da parte del Parlamento europeo e del Consiglio e l'attuazione da parte degli Stati membri della legislazione adottata. Gli obiettivi dell'Unione della sicurezza possono essere raggiunti in modo ottimale anche attraverso una stretta collaborazione con le iniziative dell'UE ad essa collegate in settori quali la sicurezza energetica, l'Unione europea della salute e il piano d'azione per la democrazia europea. La Commissione continua a contribuire con tre proposte adottate insieme alla presente relazione, riguardanti il traffico di beni culturali e l'intelligence essenziale offerta dalle informazioni anticipate sui passeggeri[5], e una proposta per contrastare la tratta di esseri umani[6].

2. PROTEZIONE DELLE INFRASTRUTTURE FISICHE E DIGITALI DAGLI ATTACCHI FISICI, INFORMATICI E IBRIDI

Protezione delle infrastrutture critiche dell'UE dagli attacchi fisici e digitali

Già prima dei recenti attacchi alle infrastrutture critiche l'UE stava consolidando la propria resilienza attraverso due iniziative collegate: la direttiva rivista[7] relativa a misure per un

---

1 COM(2020) 605 final.

2 Relazione dell'ENISA sul panorama delle minacce 2022.

3 1) Un ambiente della sicurezza adeguato alle esigenze del futuro, 2) affrontare le minacce in evoluzione, 3) proteggere gli europei dal terrorismo e dalla criminalità organizzata, 4) un forte ecosistema europeo della sicurezza.

4 La tabella allegata fornisce una panoramica delle azioni legislative e non legislative dall'avvio della strategia per l'Unione della sicurezza.

5 Piano d'azione sul traffico di beni culturali (COM(2022) 800 final) e due proposte di riesame della direttiva riguardante le informazioni anticipate sui passeggeri (COM (2022) 729 final e 731 final).

6 L'adozione della proposta di revisione della direttiva anti-tratta (COM(2022) 732 final) e della quarta relazione sui progressi compiuti nella lotta contro la tratta di esseri umani è prevista per il 19 dicembre 2022.

7 Proposta di revisione della direttiva (UE) 2016/1148.

livello comune elevato di cibersicurezza nell'Unione **(direttiva sulla sicurezza delle reti o "NIS 2")**[8] e una nuova direttiva sulla resilienza dei soggetti critici **(direttiva sulla resilienza dei soggetti critici o "direttiva CER")**[9]. Nel suo complesso, questo quadro affronta i rischi attuali e futuri, online e offline, a partire dagli attacchi informatici fino alle catastrofi naturali. Tali direttive sono state approvate dai colegislatori ed entreranno in vigore nelle prossime settimane. La **direttiva NIS 2** aumenterà la copertura dei soggetti di medie e grandi dimensioni in una serie di settori chiave[10]. Essa rafforza i requisiti di sicurezza, in particolare per quanto riguarda la risposta agli incidenti e la gestione delle crisi, la sicurezza della catena di approvvigionamento, la gestione e la divulgazione delle vulnerabilità, la sperimentazione in materia di cibersicurezza e l'uso efficace della cifratura. Semplifica inoltre gli obblighi di segnalazione degli incidenti, introduce misure di vigilanza più rigorose e mira ad armonizzare i regimi sanzionatori in tutti gli Stati membri[11]. La **direttiva CER** riguarda la resilienza fisica dei soggetti critici nei confronti dei rischi di origine umana e naturale. La direttiva, che contempla 11 settori, rappresenta un passo importante per migliorare la capacità dei soggetti critici che forniscono servizi essenziali di prevenire gli incidenti, di proteggersi, di rispondervi, di resistervi, di mitigarli, assorbirli, di adattarvisi e di riprendersi.

Nel settore **finanziario** è stato adottato, nell'ambito del pacchetto sulla finanza digitale, l'atto sulla resilienza operativa digitale (DORA)[12], che una volta approvato rafforzerà la resilienza operativa digitale delle entità del settore finanziario dell'UE, razionalizzando e aggiornando le norme vigenti e introducendo nuove prescrizioni laddove necessario.

Per aumentare ulteriormente la protezione delle **infrastrutture critiche dai ciberattacchi su vasta scala**, la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS[13] stanno elaborando **scenari di rischio** incentrati sulla cibersicurezza nei settori dell'energia, delle telecomunicazioni, dei trasporti e dello spazio. Sono inoltre in corso attività relative a misure volte a migliorare il livello collettivo di protezione e ciberresilienza dei sistemi e dei servizi spaziali[14], e valutazioni mirate dei rischi di cibersicurezza per le infrastrutture e le reti di comunicazione nell'UE (comprese le infrastrutture fisse e mobili, i satelliti, i cavi sottomarini, l'instradamento in internet)[15]. La Commissione ha inoltre avviato un'iniziativa per l'elaborazione di scenari sulle **catastrofi naturali legate a minacce per la sicurezza** come gli attacchi informatici o il terrorismo, al fine di migliorare la prevenzione, la preparazione e la risposta alle catastrofi.

---

8 COM(2020) 823 final.

9 COM(2020) 829 final.

10 I settori disciplinati dalla direttiva NIS 2 e dalla direttiva CER sono i seguenti: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, infrastrutture digitali, settore sanitario, acqua potabile, acque reflue, pubblica amministrazione, spazio e produzione, trasformazione e distribuzione di alimenti.

11 Sono in corso discussioni tra gli esperti nazionali in seno al gruppo di cooperazione NIS per sostenere gli Stati membri nel recepimento e nell'attuazione della direttiva NIS 2.

12 COM(2020) 595 final. L'accordo politico è stato raggiunto a maggio 2022.

13 Il gruppo, composto da rappresentanti degli Stati membri, della Commissione e dell'Agenzia dell'UE per la cibersicurezza (ENISA), è incaricato di sostenere e facilitare la cooperazione strategica tra gli Stati membri sulla sicurezza delle reti e dei sistemi informativi.

14 Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, 23 maggio 2022.

15 In linea con l'appello lanciato a Nevers a favore del rafforzamento delle capacità di cibersicurezza dell'Unione, concordato in occasione dell'incontro informale dei ministri delle telecomunicazioni del 9 marzo 2022.

Il sabotaggio dei gasdotti Nord Stream e altri incidenti recenti hanno evidenziato la minaccia per le **infrastrutture critiche dell'UE** e la necessità di intervenire con urgenza. Si sta pertanto predisponendo il quadro della direttiva CER e della direttiva NIS 2 per accelerare le misure volte a rafforzare la resilienza delle infrastrutture critiche e migliorare la preparazione e la risposta in settori chiave. Tale quadro sarà inserito in una **raccomandazione del Consiglio**[16] che consentirà di accelerare l'effettiva attuazione delle direttive. Esso offre un approccio comune per lo svolgimento di **prove di stress** sui gestori di infrastrutture critiche, a partire dal settore dell'energia, sulla base di principi comuni concordati. I lavori relativi alle prove di stress inizieranno immediatamente, in modo da poter essere completati entro la fine del 2023; i progressi saranno esaminati ad aprile 2023. La Commissione elaborerà, in cooperazione con il Consiglio e sulla base del sostegno e dei contributi delle pertinenti agenzie dell'Unione, un piano per garantire una risposta coordinata a livello dell'UE alle gravi perturbazioni delle infrastrutture critiche.

Nel **settore dell'energia** la Commissione sta lavorando a un codice di rete sulla cibersicurezza per i flussi transfrontalieri di energia elettrica[17], che comprende norme in materia di valutazione dei rischi, requisiti minimi comuni, pianificazione, monitoraggio, comunicazione e gestione delle crisi, che sarà pienamente coerente con il quadro NIS 2. Un'azione separata del marzo 2022 in risposta all'aggressione della Russia nei confronti dell'Ucraina ha sincronizzato le reti elettriche dell'Ucraina e della Repubblica di Moldova con la rete dell'Europa continentale, integrando le misure di attenuazione dei rischi, anche in materia di cibersicurezza.

Nel **settore dei trasporti** la Commissione collabora con gli Stati membri, l'Agenzia dell'Unione europea per la sicurezza aerea (AESA) e il Centro UE di situazione e di intelligence (INTCEN) al fine di valutare periodicamente il livello di minaccia e di rischio per l'aviazione civile dell'UE rappresentato dalle zone di conflitto. Il sistema di allerta per le zone di conflitto (*Conflict Zone Alerting System*) dell'UE è stato definito una buona prassi a livello internazionale[18]. Le azioni comprendono il rilancio di un iter di valutazione dei rischi per il trasporto aereo di merci, una prima valutazione dei rischi a livello dell'UE per valutare le minacce alle quali sono esposte le navi passeggeri e un esercizio globale di mappatura dei rischi per la sicurezza dell'aviazione al fine di aggiornare la valutazione delle minacce per l'aviazione civile.

Anche le **infrastrutture critiche marittime** sono oggetto di particolare attenzione[19]. Il sistema comune per la condivisione delle informazioni sul settore marittimo, che è attualmente in fase di sviluppo e sarà pienamente operativo entro la fine del 2023, collegherà tra loro le autorità di sorveglianza marittima su base volontaria, consentendo uno scambio di informazioni quasi in tempo reale. Il Forum europeo delle funzioni di guardia costiera ha rafforzato la propria capacità di protezione dagli attacchi informatici.

---

[16] La proposta della Commissione COM(2022) 551 final è stata seguita da una raccomandazione del Consiglio adottata l'8 dicembre 2022.

[17] Come previsto dal regolamento (UE) 2019/943 sull'energia elettrica.

[18] Organizzazione per l'aviazione civile internazionale (doc. 10084, intitolato "Risk Assessment Manual for Civil aircraft Operations Over or Near Conflict Zones" 2018).

[19] Anche attraverso l'attuazione di progetti PESCO in materia di capacità e di progetti di Orizzonte 2020.

Diversi progetti di ricerca nell'ambito di **Orizzonte Europa** mirano a rendere più sicure le nostre infrastrutture digitali e a sviluppare capacità di prevenzione e attenuazione degli attacchi informatici[20].

Rafforzamento della cibersicurezza dell'UE

Il 16 dicembre 2020 la Commissione e l'alto rappresentante hanno presentato una nuova **strategia dell'UE in materia di cibersicurezza per il decennio digitale[21],** finalizzata a rafforzare la resilienza collettiva dell'Europa contro le minacce informatiche e a garantire che i cittadini e le imprese beneficino di servizi e strumenti digitali affidabili e sicuri. La strategia è stata quasi pienamente attuata.

La direttiva NIS 2 prevede l'istituzione della **rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)**[22] per favorire la gestione coordinata degli incidenti di cibersicurezza su vasta scala a livello operativo. Ciò garantirà uno scambio regolare di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'UE. La Commissione sta sviluppando un **centro di situazione e di analisi sulla cibersicurezza** per rafforzare la sua capacità interna. La Commissione sta collaborando con gli Stati membri, anche dando seguito alla sua raccomandazione relativa a un'**unità congiunta per il ciberspazio**[23], per garantire una risposta coordinata dell'UE agli incidenti informatici su vasta scala. La Commissione e l'alto rappresentante sono inoltre attivamente coinvolti nelle esercitazioni di cibersicurezza del 2022, organizzate insieme agli Stati membri[24].

Le reti e i sistemi informatici richiedono un monitoraggio e un'analisi costanti per rilevare intrusioni e anomalie in tempo reale. La Commissione ha proposto di creare una rete di **centri operativi di sicurezza** (SOC) in tutta l'UE per monitorare le reti di comunicazione e individuare gli eventi sospetti. Il potenziamento dei SOC esistenti, l'istituzione di nuovi centri e il collegamento dei SOC in diversi Stati membri consentirà di intensificare le capacità di rilevamento collettivo. I centri potrebbero altresì avvalersi delle più moderne forme di intelligenza artificiale e analisi dei dati, proteggendo le reti di comunicazione civili e accelerando l'individuazione degli attacchi informatici[25].

Al fine di rafforzare la preparazione e la risposta agli incidenti informatici gravi, la Commissione ha inoltre definito un programma a breve termine per sostenere gli Stati membri

---

[20] EU-CIP, per un polo europeo delle conoscenze e un banco di prova delle politiche in materia di protezione delle infrastrutture critiche, e ATLANTIS, la piattaforma di prova atlantica per la robotica nel settore marittimo: nuove frontiere per l'ispezione e la manutenzione delle infrastrutture energetiche offshore.

[21] JOIN(2020) 18 final.

[22] EU-CyCLONe è composta da rappresentanti delle autorità di gestione delle crisi informatiche degli Stati membri, con la partecipazione della Commissione nei casi in cui un incidente di cibersicurezza su vasta scala potenziale o in corso abbia o possa avere un impatto significativo sui servizi e sulle attività previsti dalla direttiva.

[23] COM(2021) 4520 final.

[24] Tra gli esempi figurano l'esercitazione di cibersicurezza (Blue OLEx), organizzata dalla Lituania e dall'ENISA, e l'esercitazione EU CyCLES (Cyber Crisis Linking Exercise on Solidarity), organizzata dalla presidenza francese.

[25] È stata avviata una prima fase con un invito a presentare proposte sul tema "Sviluppo delle capacità dei centri operativi di sicurezza", e un "Invito a manifestare interesse a partecipare ad appalti congiunti di strumenti e infrastrutture", con il Centro europeo di competenza per la cibersicurezza (ECCC), pubblicato nel novembre 2022, con un finanziamento totale dell'UE pari a 110 milioni di EUR a titolo del programma DIGITAL.

attraverso finanziamenti aggiuntivi assegnati all'ENISA, compresi test di penetrazione dei soggetti critici per individuare le vulnerabilità. Tale programma può altresì assistere gli Stati membri nella risposta agli incidenti, fornita dall'ENISA con il sostegno di fornitori privati affidabili di servizi di cibersicurezza, in seguito a incidenti gravi che colpiscano soggetti critici. Il prossimo passo consisterà nel garantire che gli Stati membri sfruttino appieno tali opportunità.

Sia i prodotti hardware che quelli software sono sempre più oggetto di **attacchi informatici**. Gli attacchi informatici sono sempre più numerosi e sofisticati e lo sfruttamento delle vulnerabilità del software rappresenta il mezzo principale. Due terzi di tutti gli incidenti segnalati ai sensi della direttiva NIS riguardano lo sfruttamento delle vulnerabilità del software. Aumenta anche l'impatto su cittadini, infrastrutture e imprese[26]. Due terzi di tutti gli incidenti segnalati ai sensi della direttiva NIS riguardano lo sfruttamento delle vulnerabilità del software. A settembre 2022 la Commissione ha proposto la **legge sulla ciberresilienza**[27], diretta a ridurre le vulnerabilità nei prodotti con elementi digitali e garantire la pronta disponibilità di patch e misure di attenuazione. Essa propone che i prodotti con elementi digitali (hardware e software) entrino nel mercato solo se soddisfano specifici requisiti essenziali di cibersicurezza[28]. I fabbricanti e gli sviluppatori sarebbero tenuti a garantire la cibersicurezza dei loro prodotti per un periodo di cinque anni e ad essere trasparenti nei confronti dei consumatori in merito alla cibersicurezza. Ciò contribuirà in modo significativo alla sicurezza della catena di approvvigionamento[29].

La **certificazione** svolge un ruolo cruciale nell'accrescere la sicurezza di prodotti e servizi importanti per il mondo digitale e la fiducia in tali prodotti e servizi. Il regolamento sulla cibersicurezza[30] istituisce il quadro europeo di certificazione della cibersicurezza nell'ambito del quale la Commissione può chiedere all'ENISA di sviluppare sistemi di certificazione. È stato sviluppato un sistema europeo di certificazione della cibersicurezza basato sui criteri comuni e sono in preparazione sistemi per i servizi cloud e la sicurezza del 5G.

La Commissione continua a collaborare con gli Stati membri per garantire che le **reti 5G** siano sicure e resilienti e per monitorare l'attuazione del pacchetto di strumenti dell'UE per il 5G a livello nazionale e dell'UE. Sebbene la stragrande maggioranza degli Stati membri abbia già rafforzato o stia rafforzando i requisiti di sicurezza per le reti 5G, è ora urgente che tutti gli Stati membri completino l'attuazione delle misure del pacchetto di strumenti[31], in particolare che adottino restrizioni nei confronti dei fornitori ad alto rischio, considerando che i ritardi possono aumentare la vulnerabilità delle reti nell'Unione, e rafforzino la protezione fisica e non fisica delle parti critiche e sensibili delle reti 5G, anche tramite rigorosi controlli dell'accesso.

---

[26] Relazione dell'ENISA sul panorama delle minacce 2022.

[27] COM(2022) 454 final.

[28] Nel frattempo, a ottobre 2021 la Commissione ha adottato un regolamento delegato nell'ambito della direttiva sulle apparecchiature radio che impone ai fabbricanti di dispositivi senza fili l'obbligo di migliorare il livello di cibersicurezza, la tutela della vita privata e la protezione dalle frodi.

[29] In linea con le conclusioni del Consiglio sulla sicurezza della catena di approvvigionamento delle TIC del 17 ottobre 2022.

[30] Regolamento (UE) 2018/881, che introduce un quadro di certificazione della cibersicurezza a livello dell'UE per i prodotti, i servizi e i processi TIC.

[31] Gli Stati membri, con il sostegno della Commissione e dell'ENISA, hanno pubblicato all'inizio di quest'anno una relazione sulla cibersicurezza delle reti di accesso radio aperte, che, quando saranno più sviluppate, offriranno un modo alternativo di utilizzare la parte relativa all'accesso radio delle reti 5G sulla base di interfacce aperte.

Per aiutare l'UE e gli Stati membri ad adottare un approccio proattivo e strategico alla politica industriale in materia di cibersicurezza, il **Centro europeo di competenza per la cibersicurezza** collaborerà con i centri nazionali di coordinamento per sostenere l'innovazione in materia di cibersicurezza e rafforzare le capacità della comunità tecnologica della cibersicurezza[32].

A settembre 2022 l'ENISA ha formalmente istituito un **quadro europeo per le competenze in materia di cibersicurezza** che individua i profili professionali più necessari nel settore e fornisce una base comune europea per facilitare il riconoscimento delle competenze e sviluppare la formazione in materia di cibersicurezza. Tale quadro costituirà una base fondamentale dell'**Accademia per le competenze in materia di cibersicurezza** proposta nell'ambito del programma di lavoro della Commissione per il 2023, che offrirà un approccio globale per far fronte alla crescente necessità di professionisti della cibersicurezza in Europa.

Le istituzioni, gli organi e gli organismi dell'UE trattano informazioni sensibili non classificate e classificate che è importante proteggere adeguatamente dagli attacchi informatici. A marzo 2022 la Commissione ha proposto un regolamento per un livello comune elevato di cibersicurezza in tutti questi organismi[33], applicando i principi su cui si basa la direttiva NIS 2 al contesto istituzionale dell'UE. Il regolamento prevede un nuovo comitato interistituzionale per la cibersicurezza e un centro per la cibersicurezza rafforzato (CERT-UE)[34] destinati a garantire un adeguato scambio di informazioni e una cooperazione con le autorità degli Stati membri, ad esempio attraverso la rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT). Parallelamente la Commissione ha adottato una proposta di regolamento sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'UE[35], al fine di aumentare la resilienza contro le minacce informatiche e ibride creando un insieme comune di norme di sicurezza delle informazioni di livello elevato per tutte le istituzioni, gli organi e gli organismi dell'Unione. È essenziale che il Consiglio acceleri i lavori su tale proposta, considerando i molteplici inviti degli Stati membri che chiedono alla Commissione di elaborare misure volte a proteggere meglio il processo decisionale dell'UE da attività nocive di qualsiasi tipo. CERT-UE e l'ENISA hanno inoltre progettato e testato un nuovo tipo di esercitazione di cibersicurezza su misura per le agenzie dell'UE, come raccomandato dalla Corte dei conti europea.

Alcuni dei risultati principali

Mese europeo della cibersicurezza (ECSM): l'iniziativa ECSM, che comprende seminari, campagne sui social media e conferenze, è passata da 184 attività nel 2014 a 500 attività a ottobre 2022. Tali attività contribuiscono a migliorare la risposta degli utenti online quando devono affrontare una minaccia per la cibersicurezza (come riferito dal 73 % degli Stati membri intervistati nel 2021).

Banca dati dell'istruzione superiore sulla cibersicurezza (CyberHEAD): negli ultimi due anni CyberHEAD è stata la pagina web più visitata dell'ENISA, registrando circa 70 000 visite l'anno. Essa consente ai giovani talenti di prendere decisioni informate in merito alle varie possibilità offerte dall'istruzione superiore in materia di cibersicurezza e aiuta le università ad attrarre studenti di alta qualità motivati a mantenere l'Europa sicura dal punto di vista informatico.

32 Il consiglio di direzione dell'ECCC è in carica e la sua quarta riunione si è tenuta il 20 ottobre 2022.

33 COM(2022) 122 final.

34 CERT-UE ha investito in modo significativo nell'ulteriore miglioramento dei servizi che presta alle istituzioni, agli organi e agli organismi dell'UE e nell'integrazione di nuovi servizi, al fine di prevenire, individuare e rispondere meglio agli attacchi informatici.

35 COM(2022) 119 final.

Contrasto delle minacce ibride, lotta alle ingerenze straniere e rafforzamento della ciberdifesa dell'UE

La **bussola strategica dell'UE** per la sicurezza e la difesa delinea un ambizioso piano d'azione per aumentare la capacità di azione dell'UE, rafforzare la resilienza e investire meglio nelle capacità di difesa dell'UE.

Sebbene la lotta alle **minacce ibride** sia prevalentemente di competenza degli Stati membri, l'UE integra le azioni nazionali sostenendo il coordinamento, rafforzando la conoscenza situazionale, promuovendo la cooperazione con paesi e organizzazioni internazionali che condividono gli stessi principi e fornendo opzioni di risposta congiunta. Nell'ultimo decennio sono state predisposte oltre 200 misure per rafforzare la resilienza e contrastare le minacce ibride a livello dell'UE. La cellula dell'UE per l'analisi delle minacce ibride dell'INTCEN contribuisce al processo decisionale dell'UE ed è l'organo centrale incaricato di fornire una conoscenza situazionale globale e una previsione strategica, aggregare informazioni provenienti da tutte le fonti e condurre valutazioni di intelligence sulle minacce ibride. Sono iniziati i lavori per la creazione di gruppi di risposta rapida dell'UE alle minacce ibride, come annunciato dalla bussola strategica, per sostenere gli Stati membri e le missioni e operazioni della politica di sicurezza e di difesa comune (PSDC), nonché i paesi partner, nella lotta contro le minacce ibride attingendo alle pertinenti competenze nazionali e dell'UE con breve preavviso, comprese, ove necessario, le competenze militari. È in preparazione un pacchetto di strumenti dell'UE contro le minacce ibride che fornirà un quadro per una risposta coordinata alle campagne ibride che interessano l'Unione e i suoi Stati membri, integrando la dimensione esterna e interna in un flusso continuo e riunendo in un unico insieme le considerazioni nazionali e dell'UE. Sono stati compiuti progressi significativi anche per quanto riguarda il rafforzamento della resilienza e il contrasto delle minacce ibride attraverso l'individuazione degli attuali parametri di riferimento settoriali per la resilienza[36]. La Commissione ha inoltre proseguito la ricerca analitica sul rafforzamento della resilienza contro le minacce ibride[37] e ha completato l'integrazione di considerazioni sulle minacce ibride nell'elaborazione delle politiche.

La pandemia della COVID-19 e la guerra intrapresa dalla Russia nei confronti dell'Ucraina hanno dimostrato come la manipolazione dell'ambiente di informazione possa incidere sull'UE e sui partner in tutto il mondo. Anche **la manipolazione delle informazioni e l'ingerenza da parte di soggetti stranieri**, finalizzate a minare la fiducia nell'UE e nell'ordine internazionale basato su regole, sono una componente sempre più importante degli attacchi ibridi. Sulla base del piano d'azione per la democrazia europea, la Commissione ha messo in atto una serie di misure e strutture concrete, tra cui il codice di buone pratiche sulla disinformazione riveduto, la legge sui servizi digitali e la proposta sulla trasparenza della pubblicità politica, attualmente in fase di negoziati interistituzionali, per contrastare la manipolazione delle informazioni e la disinformazione. Ne deriverebbero nuovi obblighi per le piattaforme e, per la prima volta, un quadro di sorveglianza giuridicamente vincolante. Inoltre, come annunciato dalla bussola strategica, in stretta cooperazione con la Commissione e gli Stati membri, il Servizio europeo per l'azione esterna (SEAE) sta sviluppando ulteriormente il **pacchetto di strumenti dell'UE contro la manipolazione delle informazioni e l'ingerenza da parte di soggetti stranieri** (pacchetto di strumenti FIMI), al fine di promuovere una risposta coordinata ai comportamenti manipolativi da parte di soggetti

[36] SWD(2022) 21 final.

[37] Minacce ibride: un ecosistema globale di resilienza, JRC130097.

stranieri[38]. Il SEAE ha inoltre continuato a rafforzare la cooperazione con partner internazionali come il meccanismo di risposta rapida del G7 e la NATO.

La Commissione condanna qualsiasi ingerenza straniera nel territorio sovrano degli Stati membri dell'UE ed è preoccupata per le segnalazioni relative a stazioni di polizia cinesi d'oltremare nell'UE, le quali, qualora le segnalazioni si rivelassero fondate, sarebbero del tutto inaccettabili. Sebbene la verifica della fondatezza di tali accuse spetti alle autorità degli Stati membri, la Commissione, con il sostegno di Europol, è pronta ad agevolare gli scambi tra gli Stati membri. La Commissione ha sollevato la questione in occasione del Consiglio "Giustizia e affari interni" di dicembre 2022.

A novembre 2022 la Commissione e l'alto rappresentante hanno presentato una nuova politica di **ciberdifesa**[39] dell'UE, che definisce i mezzi per rafforzare la cooperazione e gli investimenti nella ciberdifesa al fine di migliorare la protezione dagli attacchi informatici. L'obiettivo è difendere gli interessi dell'UE nel ciberspazio rafforzando la cooperazione tra i soggetti del settore della ciberdifesa dell'UE e sviluppando meccanismi per sfruttare le capacità a livello dell'UE, anche nel contesto delle operazioni e missioni PSDC. La nuova politica promuoverà lo sviluppo di capacità di ciberdifesa a tutto spettro e rafforzerà la cooperazione tra le cibercomunità militari e civili dell'UE, migliorando la conoscenza situazionale, il coordinamento e la formazione in caso di crisi, anche con il settore privato. Contribuirà inoltre a ridurre le dipendenze strategiche dell'UE in relazione alle cibertecnologie critiche attraverso lo sviluppo di una tabella di marcia strategica per la cibersicurezza e le tecnologie critiche per la ciberdifesa, nonché a rafforzare la base industriale e tecnologica di difesa europea.

La bussola strategica considera lo **spazio** il quinto settore operativo della guerra (accanto a terra, mare, aria e ciberspazio) e chiede alla Commissione e all'alto rappresentante di sviluppare la prima strategia spaziale per la sicurezza e la difesa. La strategia proporrà misure volte a migliorare il livello collettivo di protezione e resilienza dei sistemi e dei servizi spaziali e a scoraggiare e rispondere a qualsiasi minaccia, anche informatica, posta nei confronti dei sistemi e servizi spaziali sensibili nell'UE.

3 LOTTA AL TERRORISMO E ALLA RADICALIZZAZIONE

Quasi tutte le iniziative principali presentate nell'ambito della strategia dell'UE per la sicurezza al fine di sostenere gli Stati membri nella lotta al terrorismo e alla radicalizzazione sono state adottate. Un tema che ha ricevuto particolare attenzione è quello della protezione contro le minacce online. Il prossimo passo consiste nel garantire che tali iniziative producano il massimo effetto.

[38] Sono in corso attività relative ai compiti della bussola strategica per costruire uno spazio di dati relativo alla manipolazione delle informazioni e all'ingerenza da parte di soggetti stranieri e dotare le operazioni e le missioni PSDC di capacità e risorse per l'utilizzo degli strumenti pertinenti del pacchetto di strumenti. Il SEAE continua a fornire agli Stati membri dell'UE una conoscenza situazionale open source attraverso il sistema di allarme rapido dell'UE, sensibilizza l'opinione pubblica, in particolare attraverso la campagna EUvsDisinfo, e ha ulteriormente rafforzato la sua cooperazione con portatori di interessi quali la NATO e il meccanismo di risposta rapida del G7.

[39] JOIN(2022) 49 final.

Lotta al terrorismo

Dalla sua adozione a dicembre 2020 **il programma di lotta al terrorismo dell'UE**[40] ha consentito all'UE di prevedere, prevenire, proteggere e affrontare in modo più efficace le minacce terroristiche. Iniziative geografiche specifiche hanno inoltre contribuito a reagire alla situazione di minaccia in evoluzione. Alla luce degli sviluppi in Afghanistan, il coordinatore antiterrorismo dell'UE, in coordinamento con la Commissione, l'alto rappresentante, la presidenza e le principali agenzie dell'UE, ha elaborato un **piano d'azione per la lotta al terrorismo in Afghanistan**[41], approvato dagli Stati membri a ottobre 2021. Un chiaro risultato è stata una procedura volontaria per il rafforzamento delle verifiche di sicurezza sulle persone provenienti dall'Afghanistan.

Affrontare la minaccia posta dai **combattenti terroristi stranieri di ritorno** in Siria e in Iraq rappresenta una priorità. Sebbene la responsabilità primaria spetti agli Stati membri, la cooperazione a livello dell'UE aiuta gli Stati membri ad affrontare sfide comuni quali il perseguimento di coloro che hanno commesso reati di terrorismo, la prevenzione dell'ingresso clandestino nello spazio Schengen, nonché il reinserimento e la riabilitazione dei combattenti terroristi stranieri rimpatriati. La Commissione continua a collaborare strettamente con gli Stati membri e i principali paesi partner per garantire che le prove raccolte sui campi di battaglia siano inserite nelle banche dati e nei sistemi di informazione dell'UE. D'intesa con gli Stati membri, il coordinatore antiterrorismo dell'UE sta esplorando, in stretta collaborazione con l'alto rappresentante e la Commissione, nuovi modi per promuovere migliori condizioni di vita nelle carceri e nei campi della Siria nordorientale, al fine di contribuire a combattere la radicalizzazione.

La legislazione dell'UE in materia di lotta al terrorismo è stata aggiornata. La **direttiva sulla lotta contro il terrorismo** adottata nel 2017 è ora attuata da tutti gli Stati membri[42] per qualificare come reato condotte quali l'addestramento e i viaggi a fini terroristici, nonché il finanziamento del terrorismo. Occorre affrontare ancora il problema del recepimento non corretto della direttiva in diversi Stati membri.

Privare i terroristi dei mezzi per compiere un attentato è fondamentale nella lotta contro il terrorismo. Quasi tutti gli Stati membri hanno ora adottato la legislazione aggiornata sulle armi da fuoco[43] nei rispettivi ordinamenti nazionali. A febbraio 2021 è entrata in vigore una nuova legislazione volta a limitare l'accessibilità dei precursori degli esplosivi che i terroristi potrebbero utilizzare per produrre bombe. Sulla base dell'approccio utilizzato per regolamentare l'accesso ai precursori degli esplosivi, la Commissione sta vagliando le modalità per limitare l'accesso ad alcune sostanze chimiche pericolose che potrebbero essere utilizzate per compiere attentati.

Gli **spazi pubblici** sono stati ripetutamente al centro degli attentati terroristici. La Commissione ha pubblicato un manuale per promuovere il principio della sicurezza fin dalla progettazione degli spazi pubblici[44]. La pubblicazione fa seguito a orientamenti tecnici

---

40 COM(2020) 795 final.

41 Afghanistan: piano d'azione per la lotta al terrorismo, 29 settembre 2021.

42 COM(2021) 701 final. Gli Stati membri erano tenuti a recepire la direttiva nei rispettivi quadri nazionali entro l'8 settembre 2018.

43 COM(2015) 750 final.

44 SWD(2022) 398 final.

dettagliati[45], strumenti per la valutazione delle vulnerabilità degli spazi pubblici[46] e un sostegno globale ai principali portatori di interessi[47], nonché a una raccomandazione sui requisiti di prestazione facoltativi per le apparecchiature a raggi X utilizzate negli spazi pubblici (al di fuori del settore dell'aviazione)[48]. Nel 2022 il Fondo Sicurezza interna ha inoltre stanziato 14,5 milioni di EUR per progetti volti a migliorare la protezione degli spazi pubblici, compresi i luoghi di culto. I **droni** sono uno strumento altamente innovativo che può essere utilizzato per scopi legittimi, ma anche per scopi nocivi, tra cui attacchi contro spazi pubblici, individui e infrastrutture critiche. A novembre 2022 la Commissione ha adottato una **strategia 2.0 per i droni[49]**, cui seguirà nel 2023 un approccio più dettagliato dell'UE per contrastare l'uso doloso dei droni.

Lotta alla radicalizzazione che porta all'estremismo violento e al terrorismo online e offline

Prevenire e combattere la **radicalizzazione** è fondamentale per attuare politiche antiterrorismo efficaci. La Commissione sostiene gli Stati membri con la rete di sensibilizzazione al problema della radicalizzazione (RAN) che riunisce 6 000 esperti attivi nel settore della prevenzione. Le principali aree di sostegno agli Stati membri comprendono la lotta alle ideologie estremiste violente e la polarizzazione che porta alla radicalizzazione; la radicalizzazione online e l'uso improprio delle nuove tecnologie; la gestione e la preparazione del reinserimento degli autori di reati scarcerati. I legami tra ideologie e gruppi estremisti violenti e le manifestazioni di incitamento all'odio sono affrontati nel codice di condotta dell'UE per lottare contro le forme illegali di incitamento all'odio online[50].

L'UE si sta inoltre adoperando per prevenire influenze e finanziamenti stranieri a sostegno di opinioni radicali/estremiste negli Stati membri. Da parte sua, la Commissione vigila per impedire che i fondi dell'UE sostengano progetti incompatibili con i valori europei o che perseguono un programma illegale. A tale riguardo, dalla fine del 2021 i progetti gestiti dalla Commissione sono pubblicati, subito dopo la sottoscrizione della convenzione di sovvenzione, in una piattaforma unica denominata "Funding and Tenders opportunities" (opportunità di finanziamento e appalti). È essenziale che gli Stati membri utilizzino tale piattaforma per selezionare autonomamente i beneficiari e fornire alla Commissione tutte le informazioni supplementari a loro disposizione. In tale contesto la proposta di revisione del regolamento finanziario presentata dalla Commissione prevede l'aggiunta della condanna per incitamento all'odio ai motivi di esclusione dai finanziamenti dell'UE. La Commissione invita il Parlamento europeo e il Consiglio ad affrontare in modo efficace tale questione nel testo finale. Inoltre la Commissione sta adottando misure interne di sensibilizzazione e sviluppando metodi di lavoro interni al fine di garantire un maggiore controllo nella selezione dei progetti.

---

45 Orientamenti - Protezione del perimetro degli edifici, EUR 30346 EN.

46 http://counterterrorism.jrc.ec.europa.eu.

47 Cfr. in particolare: Autumn School digitale dell'UE, JRC127168 e banca dati sul terrorismo e l'estremismo - Guida per l'uso, JRC130461.

48 Tale legge raccomanda agli Stati membri di conformarsi ai requisiti di prestazione dell'UE nell'acquisizione di apparecchiature a raggi X per l'individuazione delle minacce negli spazi pubblici (C(2022) 4179).

49 COM(2022) 652 final.

50 https://ec.europa.eu/commission/presscorner/detail/it/IP_16_1937.

Un altro obiettivo fondamentale è la prevenzione della radicalizzazione online. Il **regolamento relativo al contrasto della diffusione di contenuti terroristici online**[51] è divenuto applicabile a giugno 2022. Da allora le autorità nazionali competenti possono esigere che i contenuti terroristici siano rimossi entro un'ora dal ricevimento di un ordine di rimozione ufficiale. I fornitori di servizi online esposti a contenuti terroristici devono adottare misure specifiche per proteggere le proprie piattaforme dagli abusi. Ciò integra il lavoro del **Forum dell'UE su Internet** creato dalla Commissione per riunire gli Stati membri, le imprese di Internet e la società civile al fine di prevenire la diffusione di contenuti online legati all'estremismo estremo e al terrorismo. Il recente sostegno fornito dal Forum dell'UE su Internet alle imprese tecnologiche e ai fornitori di infrastrutture Internet nei loro sforzi di moderazione dei contenuti comprende un elenco dei siti web gestiti da terroristi e un pacchetto di conoscenze aggiornato annualmente su gruppi, simboli e manifesti dell'estremismo violento di destra[52]. Dal 2019 il Forum si occupa anche della prevenzione degli abusi sessuali online sui minori.

Alcuni dei risultati principali

In che modo la cooperazione con Eurojust ha portato alla condanna per terrorismo di un combattente straniero: il principale soggetto sottoposto a un'indagine per reati di terrorismo è stato condannato nel 2021 a quattro anni di reclusione per partecipazione a un'organizzazione terroristica dopo che le autorità italiane hanno utilizzato il registro antiterrorismo per individuare i collegamenti tra un presunto combattente straniero e altri casi di terrorismo. Eurojust ha riunito le autorità nazionali, il che ha determinato l'esecuzione degli ordini europei di indagine e delle richieste di assistenza giudiziaria reciproca.

Coordinamento di Europol contro i manuali sulle bombe disponibili online: nell'ambito di una serie di iniziative congiunte periodiche, una giornata di azione a febbraio 2022, sostenuta da Europol con la partecipazione di otto Stati membri e del Regno Unito, ha consentito di individuare centinaia di elementi online, tra cui istruzioni su come fabbricare bombe con l'ausilio di precursori e come utilizzarle negli attentati terroristici. Le informazioni sono state trasmesse ai fornitori di servizi online.

4. LOTTA ALLA CRIMINALITÀ ORGANIZZATA

Nel panorama della criminalità organizzata in Europa la cooperazione tra i criminali è in continua evoluzione. Le reti criminali possono essere coinvolte in molteplici attività criminali, che combinano traffico di stupefacenti, reati organizzati contro il patrimonio, frode, traffico di migranti e tratta di esseri umani[53]. La cibercriminalità e la violenza di genere online sono state ulteriormente stimolate dal maggiore utilizzo di Internet e dei servizi online. Il crescente ricorso a canali di comunicazione cifrati, abbinato alla necessità di tutelare la vita privata e i diritti fondamentali, pone ulteriori sfide per le autorità di contrasto[54]. Nel frattempo la perturbazione causata dalla guerra di aggressione intrapresa dalla Russia nei confronti

[51] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online (GU L 172 del 17.5.2021, pag. 79).

[52] Tra i successi realizzati figurano: un aggiornamento del protocollo di crisi dell'UE; manuali con linee guida sull'uso doloso di contenuti borderline e di videogiochi che portano alla radicalizzazione; e uno studio sugli effetti dell'amplificazione algoritmica del percorso che conduce gli utenti alla radicalizzazione.

[53] Europol (2021), valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità nell'Unione europea - "Un'influenza corruttiva: l'infiltrazione e il pregiudizio dell'economia e della società europee ad opera della criminalità organizzata", Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo.

[54] Valutazione della minaccia della criminalità organizzata su internet (IOCTA), 2021.

dell'Ucraina ha creato nuove opportunità, prontamente sfruttate dai gruppi della criminalità organizzata.

Ad aprile 2021 la Commissione ha adottato la **strategia dell'UE per la lotta alla criminalità organizzata 2021-2025**[55], che sottolinea l'importanza di smantellare le strutture della criminalità organizzata, concentrandosi sui gruppi che rappresentano un rischio maggiore per la sicurezza dell'Europa e sugli individui ai vertici delle organizzazioni criminali. L'attuazione della strategia è ben avviata: diverse azioni principali sono state già adottate o attuate. La Commissione sta inoltre fornendo un sostegno finanziario agli Stati membri per combattere le minacce della criminalità cui l'UE deve far fronte[56].

Cibercriminalità

L'accelerazione della digitalizzazione durante la pandemia della COVID-19 ha favorito la diffusione di minacce informatiche come il ransomware[57]. Il **ransomware** presenta notevoli rischi di cibersicurezza per le infrastrutture critiche e la sicurezza pubblica. Il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, in collaborazione con la task force di azione congiunta contro la criminalità informatica (J-CAT), ha recentemente sviluppato il modello internazionale di risposta al ransomware per rendere operativa una risposta globale delle autorità di contrasto. L'UE ha partecipato al vertice del 2022 dell'iniziativa "Counter Ransomware" per rafforzare la cooperazione internazionale in materia di ransomware. 36 paesi e l'UE hanno convenuto di portare avanti i lavori sulla Task Force internazionale "Counter Ransomware" per coordinare le attività sulla resilienza e le perturbazioni e contrastare il finanziamento illecito[58]. La Commissione ed Europol hanno istituito congiuntamente una piattaforma di decrittografia[59], riducendo il tempo necessario per l'accesso forense alle prove digitali e contribuendo a contrastare le reti di comunicazione criminale criptate, in modo tale da assestare un duro colpo alle attività della criminalità organizzata.

L'UE è stata determinante per il successo dei negoziati sul secondo protocollo addizionale alla **convenzione di Budapest sulla criminalità informatica** a maggio 2022. Sono stati messi in atto gli strumenti indispensabili per la cooperazione transfrontaliera nelle indagini e nel perseguimento della cibercriminalità, con condizioni e salvaguardie dettagliate in materia di protezione dei dati. Tutti gli Stati membri dovrebbero firmare in tempi brevi il secondo protocollo addizionale e il Parlamento europeo è invitato a dare la sua approvazione al fine di consentire una rapida ratifica. La Commissione sta inoltre negoziando, a nome dell'UE, una nuova convenzione delle Nazioni Unite sulla criminalità informatica.

Gli 85 milioni di immagini e video segnalati nel mondo nel solo 2021 che ritraggono **abusi sessuali sui minori**, a fronte di molti più casi non segnalati, dimostrano quanto questo fenomeno dilaghi a livelli allarmanti. I minori trascorrono più tempo online, il che li rende più vulnerabili all'adescamento e, di conseguenza, determina l'aumento dei materiali di

---

[55] COM(2021) 170 final.

[56] A luglio 2022 la Commissione ha stanziato, attraverso il Fondo Sicurezza interna (ISF), 15,7 milioni di EUR a favore degli Stati membri per sostenere progetti e attività a lungo termine nell'ambito della piattaforma multidisciplinare europea di lotta alle minacce della criminalità (EMPACT), che affronta le 10 priorità dell'UE in materia di lotta alla criminalità adottate dal Consiglio per il periodo 2022-2025.

[57] Relazione di valutazione della minaccia della criminalità organizzata su internet (IOCTA).

[58] Iniziativa internazionale "Counter Ransomware" 2022, Washington DC, 1º novembre 2022.

[59] La piattaforma di decrittografia di Europol è ospitata dal sito di Ispra del Centro comune di ricerca della Commissione europea.

sfruttamento autoprodotti. In linea con la strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori adottata a luglio 2020[60] e la strategia globale dell'UE sui diritti dei minori di marzo 2021[61], a maggio 2022 la Commissione ha adottato una proposta che stabilisce norme per la prevenzione e la lotta contro gli abusi sessuali online sui minori[62], con nuovi obblighi per i fornitori di servizi online. Laddove la prevenzione non consenta di ridurre un rischio significativo, i prestatori di servizi potrebbero essere tenuti a individuare, segnalare, rimuovere e bloccare gli abusi sessuali online sui minori. La proposta istituirebbe inoltre un apposito centro dell'UE per agevolarne l'attuazione. La legislazione temporanea adottata ad agosto 2021 per consentire ai fornitori di servizi online di continuare a individuare e segnalare volontariamente abusi sessuali online sui minori[63] scadrà nell'estate del 2024. È pertanto essenziale che il Parlamento europeo e il Consiglio raggiungano rapidamente un accordo sulla proposta di regolamento. All'inizio del prossimo anno tale iniziativa sarà integrata da una proposta di aggiornamento della direttiva del 2011 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile[64].

La violenza online contro le donne e le ragazze è una nuova dimensione emergente della **violenza di genere online**. Si stima che nel 2020 una giovane donna su due abbia subito questa forma di violenza[65]. Nella sua proposta di direttiva sulla lotta alla violenza contro le donne e alla violenza domestica[66], adottata a marzo 2022, la Commissione ha proposto norme mirate sulla violenza di genere contro le donne online o offline[67].

Criminalità organizzata

La **tratta di esseri umani** è una delle attività centrali della criminalità organizzata nell'UE[68]. Sebbene il problema sia già stata segnalato come prioritario nella strategia per l'Unione della sicurezza, i criminali hanno trovato nuove opportunità per generare profitti significativi e intensificare le attività criminali durante la pandemia della COVID-19. Un rapido coordinamento a livello dell'UE sta contribuendo a prevenire l'intensificarsi della minaccia della tratta di esseri umani a seguito della guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina. Il coordinatore anti-tratta dell'UE ha elaborato un **piano comune anti-tratta**[69] per unificare le attività della Commissione con quelle degli Stati membri, delle agenzie dell'UE e del servizio europeo per l'azione esterna (SEAE) al fine di affrontare i rischi di tratta di esseri umani e fornire un sostegno alle potenziali vittime. Tali sforzi hanno contribuito a limitare il numero di casi confermati di tratta, anche se la minaccia rimane elevata.

---

60 COM(2020) 607 final.
61 COM(2021) 142 final.
62 COM(2022) 209 final.
63 COM(2020) 568 final.
64 Direttiva 2011/93/UE, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile (GU L 335 del 17.12.2011).
65 Servizio Ricerca del Parlamento europeo (EPRS), Contro la violenza di genere: la violenza online - Valutazione del valore aggiunto europeo, 2021.
66 COM(2022) 105 final.
67 La proposta include la criminalizzazione a livello dell'UE della condivisione non consensuale di materiale intimo, lo stalking online, le molestie online e l'istigazione alla violenza o all'odio online. A ciò si aggiungerebbe un nuovo quadro di cooperazione tra le piattaforme Internet per proteggere meglio la sicurezza online delle donne.
68 Valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità (SOCTA), 2021.
69 An Anti-Trafficking Plan to protect people fleeing the war in Ukraine (europa.eu).

Ad aprile 2021 la strategia dell'UE per la lotta alla tratta degli esseri umani 2021-2025 ha presentato un quadro d'azione globale interno ed esterno[70]. La Commissione sta dando seguito a tale documento con una imminente proposta di modifica della **direttiva anti-tratta**[71] che affronta le carenze dell'attuale quadro giuridico e lo aggiornar per tenere conto della dimensione online, cercando inoltre di ridurre la domanda. A settembre 2022 si è svolta una giornata di azione congiunta della piattaforma multidisciplinare europea di lotta alle minacce della criminalità (EMPACT) dedicata alle reti criminali che utilizzano siti web e piattaforme dei social media per reclutare vittime a fini di sfruttamento sessuale, in un primo hackathon a livello dell'UE contro la tratta di esseri umani, sostenuto da Europol ed Eurojust, con le autorità di contrasto di 20 paesi. Sono stati individuati 11 presunti trafficanti di esseri umani e 45 possibili vittime[72].

A differenza delle vittime della tratta, coloro che pagano i trafficanti per entrare irregolarmente nell'UE lo fanno volontariamente. Tuttavia l'attività dei trafficanti è criminosa, spesso mette in pericolo vite umane e può comportare ulteriori rischi per la sicurezza dell'UE. 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 e del nuovo patto sulla migrazione e l'asilo[73]. Occorrono una cooperazione e un coordinamento internazionali costanti a tutti i livelli. Procede l'attuazione del piano d'azione dell'UE contro il traffico di migranti 2021-2025[74] con l'istituzione di partenariati operativi per la lotta contro il traffico di migranti con il Marocco, il Niger e i Balcani occidentali, sostenuti dalle istituzioni, dagli organi e dalle agenzie dell'UE e dai finanziamenti dell'UE.

Il mercato degli **stupefacenti illegali**, il cui valore minimo al dettaglio è stimato a 30 miliardi di EUR, è ancora il più grande mercato criminale dell'UE e una delle principali fonti di reddito per i gruppi della criminalità organizzata, nonché una minaccia per la stabilità sociale e la salute. Nel 2021 l'azione e la cooperazione dell'UE hanno portato al sequestro di stupefacenti per un valore di 7 miliardi di EUR[75]. L'**agenda e il piano d'azione dell'UE in materia di droga 2021-2025**[76] adottati a luglio 2020 definiscono azioni concrete per intensificare l'azione a livello dell'UE, compresa la trasformazione dell'Osservatorio europeo delle droghe e delle tossicodipendenze nell'Agenzia dell'Unione europea per le questioni relative agli stupefacenti. Il mandato riveduto dell'Agenzia proposto a gennaio 2022[77] rafforzerebbe le sue capacità di monitoraggio e valutazione delle minacce e la sua capacità di reagire alle nuove sfide. Il Consiglio ha adottato un orientamento generale a giugno 2022 e sono in corso i lavori in seno al Parlamento europeo. La Commissione ha inoltre avviato la cooperazione nell'ambito del Forum dell'UE su Internet per affrontare il traffico di stupefacenti online e ha proposto una valutazione tematica Schengen specifica sul traffico di cocaina nei porti dell'UE. È stato aumentato il sostegno al Centro di analisi e operazioni contro il narcotraffico marittimo. L'UE prosegue inoltre i dialoghi politici in materia di

[70] COM(2021) 171 final.
[71] La quarta relazione sui progressi compiuti nella lotta contro la tratta di esseri umani, che sarà adottata insieme alla presente proposta, contiene informazioni approfondite sull'attuazione della strategia dell'UE dal 2019 al 2022, nonché dati fondamentali e statistiche.
[72] 20 countries spin a web to catch human traffickers during a hackathon | Europol (europa.eu)
[73] COM(2020) 609 final.
[74] COM(2021) 591 final.
[75] Relazione annuale di Eurojust per il 2021.
[76] COM(2020) 606 final.
[77] COM(2022) 18 final.

stupefacenti con i paesi terzi, con un secondo dialogo con la Cina a luglio 2022 e un nuovo dialogo con la Colombia avviato a giugno 2022.

Secondo Europol, quasi il 99 % dei proventi di reato sfugge alla **confisca** nell'UE, rimanendo nelle mani degli autori dei reati[78]. Le proposte dell'UE volte a rafforzare la lotta al riciclaggio di denaro e al finanziamento del terrorismo proposte dalla Commissione a luglio 2021 sono in fase avanzata di discussione in seno al Consiglio[79]. A maggio 2022 la Commissione ha proposto di rafforzare e modernizzare le norme dell'UE in materia di recupero e confisca dei beni[80]. La proposta è stata discussa in seno ai gruppi di lavoro del Consiglio e sono stati compiuti progressi in diversi settori.

La **Procura europea** ha appena concluso il primo anno completo di attività volte alla tutela degli interessi finanziari dell'UE. Ha ricevuto 4 006 segnalazioni di reati, ha avviato 929 indagini e ha emesso provvedimenti di congelamento per un valore totale di 259 milioni di EUR. Si stima che i casi oggetto di indagine durante i primi sette mesi di attività abbiano arrecato al bilancio dell'Unione un danno di 5,4 miliardi di EUR[81].

La Commissione sta inoltre lavorando alla preparazione del **pacchetto di strumenti dell'UE contro la contraffazione**, come annunciato nel piano d'azione sulla proprietà intellettuale[82] e sottolineato nella strategia per la lotta alla criminalità organizzata.

Oltre a danneggiare la fiducia tra lo Stato e i cittadini, la **corruzione** rappresenta una minaccia per la sicurezza. È uno strumento fondamentale per la criminalità organizzata e facilita un'ampia gamma di attività criminali, che costituisce un argomento centrale del ciclo annuale della relazione sullo Stato di diritto[83]. Sebbene alcuni Stati membri dell'UE continuino a figurare tra i paesi che conseguono i risultati migliori a livello mondiale nella lotta contro la corruzione, permangono difficoltà, in particolare per quanto riguarda le indagini e le azioni penali e l'applicazione di sanzioni per corruzione. Molti Stati membri hanno adottato misure volte a rafforzare i quadri per la prevenzione della corruzione e l'integrità, ma le risorse destinate alla lotta alla corruzione sono spesso insufficienti. La Commissione sta lavorando a un pacchetto anticorruzione per il 2023 che aggiornerà e semplificherà la legislazione in questo settore.

Il piano d'azione 2020-2025 dell'UE sul **traffico di armi da fuoco**[84] è stato adottato insieme alla strategia per l'Unione della sicurezza a luglio 2020 ed è stato seguito a ottobre 2022 da una proposta di revisione delle norme in materia di autorizzazioni all'esportazione e misure di importazione e transito per le armi da fuoco[85], con una maggiore attenzione alla digitalizzazione. Nel complesso ciò dovrebbe migliorare la tracciabilità delle armi da fuoco ad uso civile. Sono inoltre in corso attività per sostenere meglio l'Ucraina e la Repubblica di

---

78 Europol, "I reati continuano a rendere? Il recupero dei proventi di reato nell'UE – Inchiesta sulle informazioni statistiche 2010-2014", 2016.

79 COM(2021) 421 final, COM(2021) 420 final, COM(2021) 423 final, COM(2021) 422 final. A giugno 2022 è stato raggiunto un accordo politico sul regolamento sui trasferimenti di fondi ed è stato definito un orientamento generale parziale sul regolamento che istituisce l'Autorità per la lotta al riciclaggio e al finanziamento del terrorismo (ad eccezione delle disposizioni relative alle risorse e alla sede).

80 COM(2022) 245 final.

81 Prima relazione annuale della Procura europea (EPPO), 2022.

82 COM(2020) 760 final.

83 L'ultima edizione della relazione è stata adottata il 13 luglio 2022 (COM(2022) 500 final).

84 COM(2020) 608 final.

85 COM(2022) 480 final.

Moldova per quanto concerne le **armi leggere e di piccolo calibro** (SALW) nel contesto dell'aggressione russa nei confronti dell'Ucraina.

Il traffico illecito di beni culturali è un'attività lucrativa per i gruppi della criminalità organizzata e, in alcuni casi, per le parti in conflitto e i terroristi[86]. Esso incentiva pertanto la criminalità organizzata, oltre ad avere un impatto negativo sul patrimonio culturale. I criminali possono abusare anche di beni culturali acquisiti legalmente per riciclare denaro, eludere le sanzioni, evadere le imposte o finanziare il terrorismo. Al fine di potenziare la **lotta contro il traffico di beni culturali**, la Commissione adotta oggi un piano d'azione[87].

Secondo Interpol e il programma delle Nazioni Unite per l'ambiente, la **criminalità ambientale** è la quarta attività criminale più importante al mondo dopo il traffico di stupefacenti, la tratta di esseri umani e la contraffazione. Sono attualmente in fase di negoziato proposte ambiziose della Commissione per una nuova direttiva sulla tutela penale dell'ambiente[88], un nuovo regolamento relativo alle spedizioni di rifiuti[89] e un nuovo regolamento sulla deforestazione[90]. Una volta adottate, tali misure rafforzeranno la catena di contrasto e permetteranno di imporre sanzioni più severe e di migliorare gli strumenti investigativi. Esse sono integrate da un piano d'azione riveduto contro il traffico illegale di specie selvatiche[91].

Alcuni dei risultati principali

EncroChat: con il sostegno di Europol e di Eurojust, le autorità giudiziarie e di contrasto di Belgio, Francia e Paesi Bassi hanno collaborato per bloccare l'utilizzo di comunicazioni cifrate da parte di gruppi della criminalità organizzata operanti su vasta scala. Al momento della sua chiusura il servizio contava 60 000 abbonati, il 90 % dei quali, secondo le stime, era costituito da criminali.

La cooperazione giudiziaria e di polizia dell'UE ha portato allo smantellamento di un gruppo della criminalità organizzata su larga scala ("caso Pollino"): una squadra investigativa comune istituita nel 2016 tra Italia, Germania e Paesi Bassi ha avviato una giornata di azione, coordinata da Eurojust e sostenuta da Europol, che ha portato alla condanna di 34 persone, per un totale di oltre 400 anni di reclusione. Successivamente altre 12 persone sono state condannate a un totale di oltre 173 anni di reclusione e i procedimenti sono ancora in corso in diversi Stati membri.

4. GARANZIA DELLA SICUREZZA DELLE NOSTRE FRONTIERE E SOSTEGNO ALLA COOPERAZIONE DELLE AUTORITÀ DI CONTRASTO E GIUDIZIARIE

Oltre ad apportare benefici economici e sociali, uno **spazio Schengen** ben funzionante è fondamentale per la sicurezza dell'UE. Occorre quindi gestire efficacemente le frontiere esterne dell'UE e rafforzare la cooperazione nell'attività di contrasto. A giugno 2021 la Commissione ha adottato una strategia per uno spazio Schengen senza controlli alle frontiere interne pienamente funzionante e resiliente[92], che definisce il modo in cui le misure sul fronte

[86] Cfr. ad esempio le risoluzioni 2199 (2015), 2253 (2015), 2322 (2016), 2347 (2017), 2462 (2019) e 2617 (2021) del Consiglio di sicurezza delle Nazioni Unite; dichiarazione di Roma dei ministri della Cultura del G20 del 30 luglio 2021.
[87] COM(2022) 800 final.
[88] COM(2021) 851 final.
[89] COM(2021) 709 final.
[90] COM(2021) 706 final.
[91] COM(2022) 581 final.
[92] COM(2021) 277 final.

della sicurezza, della cooperazione di polizia e giudiziaria possono garantire che l'UE rimanga forte contro le minacce alla sicurezza, anche senza controlli alle frontiere interne. La strategia è ora portata avanti attraverso un ciclo Schengen annuale (un nuovo modello di governance per lo spazio Schengen) i cui progressi sono registrati nella prima relazione sullo stato di Schengen, adottata a maggio 2022[93]. Un passo fondamentale è la modifica del codice frontiere Schengen[94] tramite la proposta presentata dalla Commissione nel dicembre 2021, che comprendeva nuove disposizioni a sostegno di un'efficace cooperazione in materia di sicurezza e le misure da adottare per gestire le frontiere esterne in modo più efficiente in situazioni di crisi. Alla luce di un orientamento generale del Consiglio del giugno 2022, è importante che il Parlamento europeo e il Consiglio concludano rapidamente i negoziati. La Commissione ha inoltre sottolineato i vantaggi dell'inclusione di Bulgaria, Romania e Croazia in tutti gli aspetti di Schengen, per rafforzare la sicurezza e la fiducia reciproca nello spazio Schengen[95]. A dicembre 2022 il Consiglio ha adottato una decisione sulla piena applicazione dell'*acquis* di Schengen in Croazia[96].

In uno spazio senza controlli alle frontiere interne i funzionari di polizia di uno Stato membro dovrebbero avere accesso alle stesse informazioni dei loro colleghi di un altro Stato membro. Di norma essi dovrebbero operare all'insegna di una cooperazione piena ed efficace. Per questo motivo è essenziale rafforzare gli strumenti a disposizione delle autorità di contrasto e giudiziarie in tutta l'UE per lo **scambio di informazioni e la cooperazione transfrontaliera**. Il pacchetto sulla cooperazione di polizia del dicembre 2021[97] ha offerto un importante potenziamento degli strumenti disponibili. È stato ora raggiunto un accordo politico tra il Parlamento europeo e il Consiglio in merito alla **direttiva relativa allo scambio di informazioni** e a giugno 2022 il Consiglio ha adottato una raccomandazione che rafforza le operazioni di cooperazione transfrontaliera tra le forze di polizia. Proseguono i negoziati su un regolamento che rivede il quadro Prüm[98], al fine di consentire uno scambio automatizzato di dati più efficiente tra le autorità di contrasto in settori specifici quali profili DNA, dati dattiloscopici e dati di immatricolazione dei veicoli, e di aggiungere le categorie "estratti del casellario giudiziale" e "immagini del volto". Un rapido accordo sul **regolamento Prüm II** farebbe sì che l'intera gamma di nuovi strumenti per lo scambio di informazioni diventi una realtà concreta nell'attività di contrasto negli Stati membri.

Al fine di combattere più efficacemente la criminalità transfrontaliera, i sistemi giudiziari e di contrasto degli Stati membri devono funzionare di concerto con il sostegno di agenzie dell'UE quali Europol ed Eurojust. Il nuovo mandato di **Europol** è entrato in vigore a giugno 2022, consentendo all'agenzia di rafforzare le competenze e capacità operative per sostenere meglio gli Stati membri nella lotta contro la criminalità organizzata e le forme gravi di criminalità e il terrorismo. Il mandato rafforza inoltre il quadro per la protezione dei dati di Europol e la supervisione del Garante europeo della protezione dei dati. Le autorità inquirenti e giudicanti dei diversi Stati membri devono cooperare e sostenersi reciprocamente nelle indagini e nel perseguimento dei reati e poter scambiare informazioni ed elementi di prova in modo sicuro e

[93] COM(2022) 301 final.
[94] COM(2021) 891 final.
[95] COM(2022) 636 final.
[96] A decorrere dal 1º gennaio 2023 saranno eliminate le verifiche sulle persone alle frontiere interne terrestri e marittime tra la Croazia e gli altri paesi dello spazio Schengen. I controlli alle frontiere aeree interne saranno soppressi a partire dal 26 marzo 2023.
[97] COM(2021) 782 final e COM (2021) 780 final.
[98] COM(2021) 784 final.

rapido. Il **pacchetto sulla giustizia digitale**[99] adottato a dicembre 2021 consiste in misure pratiche volte a migliorare lo scambio digitale di informazioni nei casi di terrorismo transfrontaliero, istituire una piattaforma di collaborazione come ausilio al funzionamento delle squadre investigative comuni e rafforzare la digitalizzazione della cooperazione giudiziaria e dell'accesso alla giustizia in materia civile, commerciale e penale a livello transfrontaliero. La rapida adozione del pacchetto da parte del Parlamento europeo e del Consiglio faciliterebbe notevolmente lo scambio di informazioni tra le autorità giudiziarie.

Le prove elettroniche fanno parte di quasi tutte le indagini. L'accordo politico provvisorio raggiunto a novembre 2022 sulle **prove elettroniche**[100] consentirà alle autorità giudiziarie degli Stati membri di contrastare in modo più efficace la criminalità grazie allo scambio sicuro di prove di cruciale importanza.

La **garanzia della sicurezza delle frontiere esterne dell'UE** è una responsabilità comune. Le prime squadre del corpo permanente della guardia di frontiera e costiera europea sono state dispiegate con successo a partire da gennaio 2021 e il corpo permanente conta attualmente circa 4 800 funzionari Frontex e nazionali.

L'aumento degli arrivi irregolari, che quest'anno interessa la maggior parte delle rotte migratorie, ha dimostrato l'importanza di effettuare sistematicamente controlli d'identità e verifiche di sicurezza su tutti i migranti che arrivano alle frontiere esterne dell'UE, nonché controlli dello stato di salute secondo norme comuni. La sicurezza costituisce un capitolo importante del nuovo patto sulla migrazione e l'asilo. Indirizzare rapidamente i migranti verso le procedure appropriate previste dalla **proposta relativa agli accertamenti** contribuirebbe a garantire l'applicazione delle verifiche di sicurezza, nel pieno rispetto di tutti gli obblighi in materia di diritti fondamentali. Si attende ancora una posizione del Parlamento europeo su tale proposta.

La **strumentalizzazione dei migranti** per fini politici da parte del regime bielorusso nella seconda metà del 2021 ha posto sfide giuridiche, operative e umane senza precedenti, anche per quanto riguarda la sicurezza. La proposta sul codice frontiere Schengen affronta anche la questione della strumentalizzazione dei migranti da parte di paesi terzi per fini politici. Gli Stati membri che si trovano ad affrontare tale situazione potrebbero, ad esempio, limitare il numero di valichi di frontiera e intensificare la sorveglianza di frontiera.

È in fase di sviluppo una nuova architettura dei **sistemi di informazione** dell'UE per sostenere meglio il lavoro delle autorità nazionali volto a garantire la sicurezza e la gestione delle frontiere e della migrazione. L'elemento centrale è il sistema d'informazione Schengen rinnovato, che dovrebbe divenire operativo a marzo 2023. Altri strumenti chiave sono il sistema di ingressi/uscite (la cui entrata in funzione è prevista per maggio 2023), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), che dovrebbe divenire operativo entro la fine del 2023, e l'aggiornamento del sistema di informazione visti (VIS). Ciò consentirà di intensificare le verifiche e di colmare le lacune in materia di informazioni sulla sicurezza migliorando gli scambi di informazioni tra gli Stati membri. A tal fine è fondamentale l'interoperabilità dei sistemi: è essenziale che l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) e gli Stati membri adottino senza indugio le misure necessarie affinché questo ambizioso progetto possa essere pienamente attuato entro la fine del 2024.

[99] COM(2021) 756 final, COM(2021) 757 final e COM(2021) 759 final.
[100] COM(2018) 225 final e COM(2018) 226 final.

I **controlli sulle merci in entrata** devono essere efficaci al fine di ridurre i rischi per l'UE e i suoi cittadini, garantendo nel contempo la competitività delle imprese legittime dell'UE. I controlli di sicurezza su tali merci sono stati rafforzati potenziando il sistema di controllo delle importazioni dell'UE[101], per sostenere controlli doganali efficaci basati sui rischi e misure volte a proteggere la sicurezza del trasporto aereo di merci dalle minacce terroristiche. Il programma concernente lo Strumento relativo alle attrezzature per il controllo doganale (CCEI)[102] finanzia altresì l'acquisto, la manutenzione e l'aggiornamento in condizioni di trasparenza di attrezzature per il controllo doganale pertinenti, affidabili e all'avanguardia.

La capacità delle **informazioni anticipate sui passeggeri (dati API)** di contribuire alla sicurezza è ostacolata da norme obsolete e applicate in modo disomogeneo. Le nuove proposte della Commissione abrogherebbero l'attuale direttiva API al fine di chiarire e migliorare l'utilizzo dei dati API sia per la gestione delle frontiere che per l'attività di contrasto[103]. L'uso dei dati API sarebbe esteso a voli intra-UE selezionati e sarebbe ampliato il pacchetto di strumenti a disposizione delle autorità di contrasto degli Stati membri all'interno dello spazio Schengen. Sono in corso riflessioni sulla dimensione esterna della politica dell'UE in materia di **dati del codice di prenotazione** (PNR), dato che un numero crescente di paesi terzi sta sviluppando la capacità di trattare tali informazioni per le attività di contrasto e la sicurezza delle frontiere. La Commissione sta inoltre preparando una proposta legislativa su un quadro per l'accesso reciproco alle informazioni in materia di sicurezza per i funzionari in prima linea nell'UE e nei paesi terzi partner, al fine di individuare efficacemente criminali e terroristi.

La **falsificazione dei documenti di viaggio** facilita il movimento clandestino di criminali e terroristi e svolge un ruolo fondamentale nella tratta di esseri umani e nel commercio di stupefacenti. Poiché occorre affrontare questo problema e parallelamente agevolare i viaggiatori legittimi, da agosto 2021 gli Stati membri rilasciano carte d'identità con norme di sicurezza armonizzate, compreso un chip contenente identificatori biometrici che può essere verificato da tutte le autorità di frontiera dell'UE[104]. La Commissione sta preparando un'ulteriore iniziativa sulla digitalizzazione dei documenti di viaggio e sull'agevolazione dei viaggi[105], che rafforzerà la sicurezza e accelererà le procedure di viaggio e di frontiera attraverso la comunicazione anticipata di dati di viaggio e dati personali senza supporti cartacei e i controlli biometrici alle frontiere.

Attività di contrasto e nuove tecnologie

Tecnologie quali l'**intelligenza artificiale** o la cifratura possono rappresentare un valore aggiunto per le autorità di contrasto e giudiziarie, ma possono anche ostacolarne il lavoro. Nella sua comunicazione sull'intelligenza artificiale (IA) e nella legge sull'intelligenza

[101] Il sistema di controllo delle importazioni 2 (ICS2) entrerà in funzione in tre versioni (marzo 2021, marzo 2022 e marzo 2023), ciascuna delle quali riguarda operatori economici (OE) e modalità di trasporto diversi.

[102] Regolamento (UE) 2021/1077 del Parlamento europeo e del Consiglio del 24 giugno 2021 che istituisce, nell'ambito del Fondo per la gestione integrata delle frontiere, lo Strumento di sostegno finanziario relativo alle attrezzature per il controllo doganale.

[103] COM(2022) 729 final e 731 final.

[104] Sulla base del regolamento (UE) 2019/1157 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione (GU L 188 del 12.7.2019, pag. 67).

[105] EUR-lex 52022PC0658.

artificiale[106], la Commissione ha sottolineato che l'IA può contribuire in maniera significativa agli obiettivi della strategia per l'Unione della sicurezza, contrastando le minacce attuali e prevedendo futuri rischi e opportunità[107]. Nell'ambito di Orizzonte Europa, il programma di ricerca e innovazione dell'UE per il periodo 2021-2027, sono disponibili finanziamenti per azioni di innovazione e **ricerca in materia di sicurezza civile**, compresi settori quali l'IA o la biometria. Solo per il 2021 e il 2022 sono già stati programmati 413,8 milioni di EUR[108].

Un risultato esemplare

Uso del sistema d'informazione Schengen (SIS): nel 2021 gli Stati membri hanno effettuato quasi 7 miliardi di ricerche nel SIS. Le autorità degli Stati membri hanno effettuato quasi 20 milioni di ricerche nel sistema in media al giorno, con una media giornaliera di 600 riscontri positivi (hit) relativi a segnalazioni estere, contribuendo a risolvere un numero equivalente di casi. Ad esempio, a seguito di un brutale doppio omicidio in Romania nel 2021, l'autore del reato è stato rintracciato in Italia a distanza di pochi giorni, grazie a una segnalazione per l'arresto inserita nel SIS che ha allertato gli investigatori italiani, consentendo loro di arrestare l'uomo a Roma.

5. NESSO TRA SICUREZZA INTERNA ED ESTERNA: LA SICUREZZA NEI PAESI VICINI ALL'UE E NEI PAESI PARTNER

Vi è uno stretto nesso tra ciò che accade al di fuori delle frontiere dell'UE e la sicurezza all'interno dell'Europa. Sostenere e aiutare i nostri vicini e partner a rafforzare la loro sicurezza interna e a cooperare con i nostri alleati e con organizzazioni internazionali quali la NATO e l'ONU è indispensabile per rafforzare la sicurezza interna dell'UE.

Il SEAE e i servizi della Commissione collaborano strettamente con i principali paesi partner e le organizzazioni internazionali attraverso dialoghi periodici **in materia di lotta al terrorismo**. Sono in corso oltre 30 dialoghi in materia di lotta al terrorismo con paesi terzi e organizzazioni internazionali[109]. Parallelamente è stata rafforzata la rete di esperti in materia di antiterrorismo e di sicurezza nelle delegazioni dell'UE dei principali paesi terzi.

Al fine di contrastare meglio le minacce alla sicurezza interna derivanti dalla guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina, i servizi della Commissione e il SEAE, insieme al coordinatore antiterrorismo dell'UE, hanno convenuto con l'**Ucraina** di istituire una cooperazione strutturata continuativa in materia di sicurezza. Tale collaborazione mira a potenziare la cooperazione operativa, anche con Europol e Frontex, nonché a rafforzare lo scambio di informazioni sulle minacce alla sicurezza interna. Le agenzie dell'UE hanno fornito un sostegno immediato per rispondere alle sfide poste dall'invasione. Attualmente

[106] COM(2021) 206 final.
[107] COM(2021) 205 final.
[108] Orizzonte Europa investe inoltre ingenti fondi in tecnologie innovative a vantaggio delle autorità di contrasto nella lotta alla radicalizzazione, nonché in progetti di individuazione di stupefacenti ed esplosivi, traffico di beni culturali, traffico di migranti, sicurezza degli spazi pubblici e furto di identità.
[109] Nel 2022 si sono svolti dialoghi in materia di lotta al terrorismo con le Nazioni Unite, Israele e India; altri dialoghi con Turchia, Qatar ed Emirati arabi uniti si terranno a breve. Nel 2023 i principali dialoghi previsti sono con il Marocco, la Tunisia, l'Egitto, il Kenya, gli Stati Uniti, il Regno dell'Arabia Saudita ed eventualmente anche con l'Algeria.

Frontex ha inviato nella regione 277 membri del personale, Europol 15 e l'Agenzia dell'Unione europea per l'asilo 60.

Le autorità di contrasto degli Stati membri e i loro partner collaborano nel quadro della **piattaforma EMPACT** per organizzare azioni operative e giornate di azione congiunta contro le minacce della criminalità nuove o in evoluzione connesse all'aggressione della Russia nei confronti dell'Ucraina.

Il **dialogo in materia di cibersicurezza** tra l'UE e l'Ucraina è stato intensificato con un sostegno politico, finanziario e materiale coordinato da parte dell'UE per aiutare l'Ucraina a rafforzare la sua ciberresilienza. Un finanziamento complessivo di 29 milioni di EUR finalizzato ad aumentare la resilienza informatica e digitale dell'Ucraina ha sostenuto le attrezzature e il software per la cibersicurezza, nonché la trasformazione digitale resiliente.

Data la sua posizione geografica, la Repubblica di **Moldova** ha un ruolo chiave da svolgere nell'affrontare le implicazioni criminali e di sicurezza dell'invasione dell'Ucraina da parte della Russia. A luglio 2022 la Commissione, in cooperazione con il SEAE, ha lanciato un polo di sostegno dell'UE per la sicurezza interna e la gestione delle frontiere con la Repubblica di Moldova. Il suo ruolo principale consiste nell'agevolare la cooperazione e l'azione operativa per affrontare le minacce comuni alla sicurezza in sei settori prioritari individuati congiuntamente dall'UE e dalla Repubblica di Moldova: traffico di armi da fuoco, traffico di migranti, tratta di esseri umani, prevenzione e contrasto del terrorismo e dell'estremismo violento, cibercriminalità e traffico di stupefacenti. A marzo 2022 la Repubblica di Moldova ha firmato un accordo sullo status con Frontex, sulla base del suo mandato rafforzato.

Negli ultimi tre anni ha continuato a intensificarsi la cooperazione tra l'UE e i **paesi dei Balcani occidentali** in materia di attività di contrasto, anche con il sostegno delle agenzie dell'UE. In linea con le conclusioni del Consiglio a marzo 2021, la cooperazione nell'attività di contrasto con i paesi terzi è stata integrata in tutti i piani d'azione operativi della piattaforma EMPACT; ne è conseguito un aumento della partecipazione dei Balcani occidentali alle attività della piattaforma. Lo strumento di preadesione continua a fornire finanziamenti significativi per la riforma e il miglioramento dei risultati delle autorità di contrasto, mentre le agenzie dell'UE forniscono un sostegno agli operatori della sicurezza in termini di potenziamento delle capacità. Il piano d'azione comune sulla lotta al terrorismo firmato nel 2018 ha registrato buoni progressi e, nel caso della Macedonia del Nord e dell'Albania, considerando che la maggior parte delle azioni è stata completata, a dicembre 2022 è stata firmata una versione aggiornata riveduta dei rispettivi accordi bilaterali per migliorare ulteriormente la nostra cooperazione nel settore della lotta al terrorismo e della prevenzione e del contrasto dell'estremismo violento.

Il 18 novembre 2022 il Consiglio ha autorizzato l'avvio di negoziati relativi ad **accordi sullo status di Frontex** tra l'UE e l'Albania, la Serbia, il Montenegro e la Bosnia-Erzegovina[110]. Tali accordi consentirebbero a Frontex di inviare squadre per la gestione delle frontiere per svolgere compiti di controllo di frontiera, sotto il comando delle autorità nazionali competenti. Ciò sarà particolarmente utile per contrastare il traffico di migranti.

[110] Decisione (UE) 2022/2271 del Consiglio – Albania; decisione (UE) 2022/2272 del Consiglio – Bosnia-Erzegovina; decisione (UE) 2022/2273 del Consiglio – Montenegro; decisione (UE) 2022/2274 del Consiglio – Serbia.

La Macedonia del Nord ha firmato un accordo sullo status con Frontex a ottobre 2022, in virtù del suo mandato rafforzato.

Anche **l'UE e gli USA** vantano una lunga storia di partenariato e cooperazione in materia di sicurezza, con l'obiettivo di uno scambio più sistematico e tempestivo di informazioni su questioni quali il terrorismo, la radicalizzazione e la criminalità organizzata. L'UE e gli USA tengono riunioni congiunte periodiche in materia di giustizia e affari interni per approfondire la cooperazione su questioni di interesse comune, promuovere la sicurezza globale e aggiornarsi reciprocamente sui progressi legislativi relativi ai fascicoli GAI (giustizia e affari interni). Le autorità giudiziarie e di contrasto europee collaborano strettamente con i loro omologhi statunitensi su questioni operative e legislative. Le autorità di contrasto statunitensi partecipano attivamente a diverse azioni e reti EMPACT, con un accordo di cooperazione operativa tra gli Stati Uniti ed Europol. Un eccellente esempio di cooperazione efficace è la task force operativa Greenlight/Trojan Shield, una delle più grandi e sofisticate operazioni di contrasto finora svolte nella lotta contro le attività criminali che si avvalgono di comunicazioni criptate. Il programma di controllo delle transazioni finanziarie dei terroristi (TFTP) tra l'UE e gli Stati Uniti fornisce numerose piste concrete per le indagini terroristiche[111]. La cooperazione si basa anche su un chiaro monitoraggio delle salvaguardie e dei controlli.

I dialoghi periodici UE-USA in materia di cibersicurezza rafforzano la cooperazione e il coordinamento sia in materia di diplomazia informatica che di ciberresilienza, compresa la normazione relativa alla cibersicurezza. Il Consiglio per il commercio e la tecnologia (TTC) ha inoltre consentito di approfondire la cooperazione, con una dichiarazione congiunta sulla cibersicurezza e misure per una potenziale cooperazione in materia di ricerca e sviluppo oltre il 5G e 6G, sui controlli delle esportazioni e sul controllo degli investimenti, nonché sulle sanzioni nei confronti della Russia e della Bielorussia. Il TTC porterà inoltre avanti la cooperazione UE-USA in materia di manipolazione delle informazioni e ingerenza da parte di soggetti stranieri.

I gravi problemi di sicurezza in corso in Africa incidono direttamente sugli africani stessi ma anche sulla sicurezza dell'UE. Sono in fase di attuazione numerosi progetti intesi ad aiutare i paesi partner a sviluppare le capacità necessarie per affrontare tali sfide, ad esempio attraverso il finanziamento dell'accademia internazionale per la lotta al terrorismo (*Académie Internationale de Lutte Contre le Terrorisme*, AILCT) nell'Africa occidentale o l'iniziativa regionale volta a rafforzare le capacità per contrastare il riciclaggio di denaro e il finanziamento del terrorismo nella regione del Grande Corno d'Africa.

I paesi dell'**America latina e dei Caraibi** (ALC) sono partner essenziali per l'UE: a maggio 2022 è stata avviata una nuova iniziativa regionale Team Europa per la sicurezza e la giustizia al fine di istituire un partenariato UE-ALC per il rafforzamento dello Stato di diritto e la lotta alla criminalità organizzata.

Il regolamento dell'UE sul **controllo degli investimenti esteri diretti** entrato in vigore a ottobre 2020[112] fornisce un quadro per migliorare la protezione dagli investimenti esteri diretti che presentano un rischio per la sicurezza o per l'ordine pubblico in più di uno Stato membro. Nel suo primo anno completo di attività sono stati notificati alla Commissione più di 400 casi.

[111] Cfr. la sesta verifica congiunta dell'attuazione dell'accordo TFTP, COM(2022) 585 final.
[112] (UE) 2019/452.

Il regolamento sui prodotti a duplice uso[113], adottato a settembre 2021, ha potenziato e rafforzato il sistema di **controllo delle esportazioni di prodotti a duplice uso** dell'UE e ha introdotto nuove disposizioni che consentono all'UE, in coordinamento con gli Stati membri, di effettuare controlli autonomi sulle esportazioni di prodotti e tecnologie non compresi negli elenchi.

In un mondo globalizzato in cui le forme gravi di criminalità e il terrorismo sono sempre più transnazionali, le autorità giudiziarie e di polizia dovrebbero essere dotate di tutti gli strumenti necessari per cooperare con i partner esterni al fine di garantire la sicurezza dei loro cittadini. Occorre quindi aprire la strada alla cooperazione e allo scambio di informazioni tra le autorità giudiziarie dei paesi terzi per **Europol ed Eurojust**. A un accordo firmato a giugno 2022 tra Europol e la Nuova Zelanda sullo scambio di dati personali per la lotta contro le forme gravi di criminalità e il terrorismo[114] hanno fatto seguito negoziati con una serie di altri paesi, ma nella maggior parte dei casi i progressi rimangono lenti. Per quanto concerne Eurojust, i negoziati con l'Armenia sono a buon punto ed è stato raggiunto un accordo sul testo, mentre sono stati avviati i negoziati con Colombia, Algeria e Libano.

Ad aprile 2022 l'**UE e le Nazioni Unite** hanno adottato misure concrete al fine di rafforzare il loro partenariato per combattere le minacce alla pace e alla sicurezza internazionali, persistenti ma in evoluzione, in occasione del quarto dialogo dei leader sulla lotta al terrorismo. Il partenariato strategico è stato ulteriormente rafforzato con l'avvio del nuovo "Strumento UE-ONU per le minacce terroristiche globali", un'iniziativa finanziata dall'UE per sostenere gli Stati che devono affrontare il terrorismo e l'estremismo violento, anche attraverso l'assistenza, la formazione e il tutoraggio. Tra le altre questioni di interesse comune figurano le minacce emergenti connesse alle nuove tecnologie, compreso il modo in cui esse colpiscono i giovani in quanto particolare gruppo bersaglio della radicalizzazione violenta, nonché il terrorismo basato sulla xenofobia, il razzismo e altre forme di intolleranza, o in nome della religione o del credo.

È stata rafforzata la **cooperazione UE-NATO**, con risultati tangibili in tutti gli ambiti di cooperazione[115]. L'UE e la NATO hanno intensificato le loro attività e la loro cooperazione a seguito della guerra di aggressione russa, adottando una posizione politica unificata e coordinandosi per aiutare l'Ucraina a difendersi e proteggere la popolazione. In questo momento critico per la sicurezza euro-atlantica, il partenariato strategico UE-NATO è più solido e pertinente che mai. Per quanto riguarda la resilienza, a gennaio 2022 è stato avviato un dialogo strutturato, attualmente in fase di approfondimento, per sostenere la protezione delle infrastrutture critiche, e in tale contesto sarà istituita una task force UE-NATO. Per quanto concerne la mobilità militare, sono stati apportati ulteriori miglioramenti relativi ai trasporti e agli aspetti normativi, compreso il trasporto di merci pericolose. Anche il contrasto delle minacce ibride rimane uno dei settori prioritari di cooperazione con la NATO. Gli scambi riguardano questioni quali la lotta al terrorismo, la comunicazione strategica, la manipolazione delle informazioni e l'ingerenza da parte di soggetti stranieri, nonché questioni legate al ciberspazio. Tra le esercitazioni effettuate figura la "Integrated Resolve" dell'UE del novembre 2022 nell'ambito del sistema di esercitazione parallela e coordinata (PACE), con la

[113] (UE) 2021/821 rifusione.

[114] L'accordo è stato accolto con favore dal Garante europeo della protezione dei dati (GEPD), che lo ha descritto come un modello per accordi futuri sullo scambio di dati personali a fini di contrasto.

[115] Cfr. la settima 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, 20 giugno 2022.

partecipazione del personale della NATO, al fine di migliorare l'interazione tra i rispettivi meccanismi di risposta alle crisi.

Da settembre 2022 l'UE copresiede il **Forum globale contro il terrorismo**. Tra le priorità figurano la risposta alla minaccia terroristica in Africa e l'integrazione della dimensione di genere e dell'istruzione nella politica antiterrorismo.

Sono in corso negoziati per un accordo di cooperazione tra l'Unione e **Interpol** per giungere a una conclusione a livello tecnico nel primo semestre del 2023. L'obiettivo principale è rafforzare ulteriormente lo scambio di informazioni tra Interpol e le agenzie e gli organismi dell'UE al fine di sostenere meglio gli Stati membri e aumentare la sicurezza dei cittadini, non solo nell'UE ma in tutto il mondo.

Un risultato esemplare

Operazione Desert Light: sgominato in sei paesi un cartello europeo della droga: a novembre 2022 sono stati effettuati raid coordinati in tutta Europa e negli Emirati arabi uniti, rivolti sia al centro di comando e controllo che all'infrastruttura logistica per il traffico di stupefacenti in Europa. Gli obiettivi di alto valore dei raid avevano costituito un "super cartello" che controllava circa un terzo del commercio di cocaina in Europa. Sono stati arrestati in tutto 49 indagati a seguito di indagini condotte in Spagna, Francia, Belgio, Paesi Bassi e negli Emirati arabi uniti con il sostegno di Europol. Nel corso delle indagini le autorità di contrasto hanno sequestrato 30 tonnellate di stupefacenti.

6. CONCLUSIONI

Negli ultimi due anni e mezzo la Commissione, in stretta collaborazione con il servizio europeo per l'azione esterna, ha realizzato con successo quasi tutte le azioni previste dalla strategia per l'Unione della sicurezza. Occorre procedere all'adozione e soprattutto all'attuazione dell'ampia gamma di proposte. Le decisioni e le azioni del Parlamento europeo, del Consiglio e dei singoli Stati membri saranno fondamentali per garantire che l'UE crei un solido ecosistema della sicurezza per i suoi cittadini.

Allo stesso tempo, l'ambiente della sicurezza continuerà a cambiare intorno a noi. Da quando è stata adottata la strategia per l'Unione della sicurezza, l'UE ha dovuto far fronte alla pandemia della COVID-19 e all'impatto dell'aggressione della Russia nei confronti dell'Ucraina. Sono aumentate in maniera esponenziale le minacce online, che rendono necessario adattarsi rapidamente e formulare veloci previsioni. L'UE deve continuare a dotarsi degli strumenti necessari per far fronte alle minacce in evoluzione che mettono a repentaglio la sicurezza dei suoi cittadini. La vigilanza costante, la determinazione ad agire e le risposte collettive saranno fondamentali per garantire in prospettiva il successo collettivo dell'UE.