COMMISSIONE
EUROPEA

Bruxelles, 25.5.2022
COM(2022) 252 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

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

I. INTRODUZIONE

La guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina domina l'attuale agenda dell'UE in materia di sicurezza. La guerra non solo minaccia l'Ucraina, ma punta anche a compromettere la stabilità e la sicurezza a livello mondiale. All'interno dell'UE, essa comporta una serie di rischi per la sicurezza dei cittadini. Sussistono nuove incertezze per quanto riguarda le forniture di energia e di altre materie prime e vi è la possibilità che le infrastrutture critiche siano oggetto di attacchi informatici. La sicurezza interna dell'UE è minacciata da potenziali attacchi o incidenti legati all'impiego di agenti chimici, biologici o radiologici nella zona di guerra. Le vulnerabilità di milioni di persone che sono fuggite dalla guerra possono essere rapidamente sfruttate dalla criminalità organizzata mediante la tratta di donne e bambini, che sono soggetti particolarmente a rischio.

A fronte di queste nuove potenziali minacce, l'UE è rimasta risoluta e unita. Benché sinora gli effetti della guerra siano rimasti perlopiù limitati al territorio dell'Ucraina, l'UE ha intensificato *la vigilanza e il coordinamento*, attuando un monitoraggio rafforzato del panorama delle minacce, e si è impegnata a rafforzare la resilienza per garantire la propria *preparazione* a qualsiasi eventualità.

Nella dichiarazione di Versailles del 10 e 11 marzo 2022[1], i leader europei hanno sottolineato la necessità di prepararsi alle sfide che emergono repentinamente, provvedendo anche a "proteggerci da una guerra ibrida in continua crescita, rafforzare la nostra ciberresilienza, proteggere le nostre infrastrutture – in particolare quelle critiche – e combattere la disinformazione".

Il quadro dell'Unione della sicurezza è fondamentale per garantire la sicurezza in tutta l'UE. Le quattro priorità strategiche definite nella strategia per l'Unione della sicurezza[2] rimangono direttamente pertinenti per assolvere tale compito nell'attuale contesto geopolitico: i) un ambiente della sicurezza adeguato alle esigenze future; ii) affrontare le minacce in evoluzione; iii) proteggere i cittadini europei dal terrorismo e dalla criminalità organizzata; e iv) un forte ecosistema europeo in materia di sicurezza. La guerra ha sottolineato la necessità che l'UE e i suoi Stati membri si avvalgano appieno degli strumenti legislativi e strategici già disponibili nell'ambito della strategia per l'Unione della sicurezza, che sono alla base del sostegno coordinato che l'UE offre agli Stati membri in merito a questioni che spaziano dalla criminalità organizzata e dal terrorismo alla cibersicurezza e alle minacce ibride.

Anche le agenzie europee che operano nel campo della giustizia e degli affari interni hanno intensificato i loro sforzi in risposta alla guerra in Ucraina, svolgendo un ruolo chiave nella valutazione delle minacce e nel sostegno alle risposte operative[3]. Un altro fattore importante è il costante rafforzamento del funzionamento e della governance dello spazio Schengen.

Questa quarta relazione sui progressi compiuti nella strategia dell'UE per l'Unione della sicurezza si concentra sugli sviluppi registrati negli ultimi mesi, a partire dallo scoppio della guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina. La relazione fornisce una panoramica delle azioni intraprese in tutte le componenti dell'Unione della sicurezza ed esamina le esigenze in termini di preparazione derivanti dalle potenziali minacce per la

[1] https://www.consilium.europa.eu/media/54792/20220311-versailles-declaration-it.pdf.
[2] COM(2020) 605 final.
[3] Dichiarazione comune delle agenzie dell'UE che operano nel campo della giustizia e degli affari interni sull'Ucraina |Agenzia dell'Unione europea per l'asilo (europa.eu).

sicurezza generate dalla guerra in Ucraina. I progressi compiuti in relazione ad altri fascicoli riguardanti l'Unione della sicurezza sono riportati nell'allegato.

II. CIBERSICUREZZA E INFRASTRUTTURE CRITICHE

Dallo scoppio della guerra, soggetti privati e organizzazioni criminali hanno pubblicizzato il fatto che stanno intraprendendo attività informatiche a sostegno di una parte o dell'altra. L'hacktivismo[4] rappresenta una minaccia a causa del rischio di effetti di ricaduta nell'UE ai danni di servizi critici, del rischio di attacchi provenienti da reti ufficiali o di altri effetti di ricaduta imprevisti. Benché sinora la guerra sia stata condotta in gran parte attraverso mezzi convenzionali, con effetti di ricaduta limitati, il rischio di un'escalation in questo settore è concreto.

L'UE ha pertanto intensificato il proprio coordinamento e la propria preparazione. Le minacce derivanti dalla guerra mettono in risalto la necessità di creare una cultura della condivisione delle informazioni e delle competenze tra l'UE, gli Stati membri e le comunità della cibersicurezza. A tal fine occorre sviluppare una conoscenza situazionale integrata, condivisa dalle istituzioni, dagli organismi e dalle agenzie dell'UE e dagli Stati membri, in particolare per quanto riguarda le infrastrutture critiche da cui dipende il corretto funzionamento del mercato interno.

Attribuzione degli attacchi informatici contro l'Ucraina

Gli attacchi informatici contro l'Ucraina sono iniziati prima dell'aggressione russa e durante i primi giorni di guerra[5], con l'obiettivo di compromettere gli account del personale militare ucraino e perturbare i servizi essenziali, compresi il controllo delle frontiere e le telecomunicazioni.

Il 14 gennaio 2022 l'alto rappresentante ha rilasciato una dichiarazione[6] a nome dell'Unione europea in cui condannava gli attacchi informatici contro l'Ucraina e riconfermava l'inequivocabile sostegno dell'UE a favore di quest'ultima.

Il 10 maggio l'Unione europea e i suoi Stati membri, insieme ai partner internazionali, hanno condannato[7] fermamente l'attività informatica dolosa condotta nei confronti dell'Ucraina il 24 febbraio, che ha preso di mira la rete satellitare KA-SAT, di proprietà di Viasat, e hanno attribuito direttamente l'attacco alla Federazione russa. L'attacco informatico ha avuto un impatto significativo e ha provocato interruzioni indiscriminate delle comunicazioni e perturbazioni per una serie di autorità pubbliche, imprese e utenti in Ucraina, interessando anche diversi Stati membri dell'UE.

---

4 Un esempio recente di hacktivismo è l'uso dei "*protestware*" per installare software maligni su dispositivi con indirizzi IP russi attraverso un pacchetto *open source* ampiamente diffuso, causando potenziali rischi per le catene di approvvigionamento e perdita di fiducia nella comunità *open source*. La Commissione ha chiarito che gli attacchi informatici (compresi quelli motivati da buone intenzioni) contro la Russia sono illegali.

5 Relazione speciale di Microsoft: *An overview of Russia's cyberattack activity in Ukraine*; *The hybrid war in Ukraine – Microsoft On the Issues*.

6 https://www.consilium.europa.eu/it/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/.

7 Operazioni informatiche russe contro l'Ucraina: dichiarazione dell'alto rappresentante a nome dell'Unione europea – Consilium (europa.eu).

Vigilanza e coordinamento

Da quando è in corso la guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina, il monitoraggio della situazione della cibersicurezza negli Stati membri e nelle istituzioni dell'UE è stato intensificato. L'Agenzia dell'UE per la cibersicurezza (ENISA), il Centro europeo per la lotta alla criminalità informatica di Europol, la squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie europee (CERT-UE) e il Centro UE di situazione e di intelligence (INTCEN) hanno contribuito alla conoscenza situazionale condivisa dell'UE, garantendo tra l'altro un monitoraggio costante delle attività informatiche sospette, anche in settori specifici quali l'energia, i trasporti e l'aviazione, e hanno fornito valutazioni volte a orientare l'azione preventiva.

Sono stati inoltre intensificati il coordinamento e lo scambio di informazioni con le reti di cibersicurezza, come la rete delle organizzazioni di collegamento per le crisi informatiche (CyCLONe), che comprende gli organismi nazionali competenti in materia di cibersicurezza, la Commissione e l'ENISA. Per integrare tale approccio all'interno delle istituzioni dell'UE è stata istituita la task force per le crisi informatiche, un meccanismo di coordinamento che consente lo scambio di informazioni tra tutti i servizi, gli organi e le agenzie competenti, tra cui l'ENISA, il Centro europeo per la lotta alla criminalità informatica di Europol e CERT-UE. Sono necessari sforzi costanti per garantire canali di comunicazione tra i livelli politico, operativo e tecnico, nonché per rafforzare la cooperazione con la rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT).

Europol ha inoltre attivato il protocollo di risposta alle emergenze delle autorità di contrasto dell'UE, che consente di rafforzare il monitoraggio delle minacce informatiche e la condivisione di informazioni tra un'ampia gamma di portatori di interessi al fine di elaborare un quadro completo di intelligence informatica.

Oltre alle minacce informatiche, gli Stati membri, il SEAE e i servizi della Commissione hanno intensificato la vigilanza sull'esposizione delle infrastrutture critiche alle minacce fisiche, non informatiche. Le infrastrutture critiche e i relativi gestori possono essere esposti a rischi fisici, quali il sabotaggio da parte dello Stato o di soggetti finanziati dallo Stato nell'ambito di possibili misure di ritorsione nei confronti dell'UE.

Preparazione

La preparazione nel settore della cibersicurezza e della sicurezza delle infrastrutture critiche è più che mai essenziale, data la maggiore esposizione dell'Europa a un accumulo di minacce dovute alla guerra. Gli sforzi per intensificare la preparazione hanno comportato l'avvio di una serie di azioni dirette, tra cui alcune già previste prima dell'aggressione della Russia nei confronti dell'Ucraina. Tali azioni comprendono esercitazioni, l'elaborazione di orientamenti, l'adozione di misure legislative, l'aumento della resilienza nei settori critici e la collaborazione con i partner.

La presidenza francese del Consiglio dell'Unione europea, insieme al servizio europeo per l'azione esterna (SEAE) e all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), ha organizzato all'inizio del 2022 un'esercitazione basata sulla simulazione di uno scenario, denominata "EU CyCLES" (*Cyber Crisis Linking Exercise on Solidarity*), con l'obiettivo di sensibilizzare a livello politico e rafforzare la cooperazione tra i livelli operativo e politico in caso di attacco informatico su vasta scala.

A febbraio l'ENISA e CERT-UE hanno pubblicato **orientamenti** su come aumentare la resilienza e la preparazione nell'UE[8]. Tali orientamenti esortano tutte le organizzazioni dei settori pubblico e privato dell'UE ad adottare un insieme minimo di migliori pratiche in materia di cibersicurezza per rafforzare in misura considerevole la cultura della cibersicurezza. A marzo CERT-UE ha pubblicato orientamenti tecnici di follow-up con il contributo dell'ENISA[9], nonché orientamenti in materia di sicurezza per rafforzare la configurazione delle app Signal[10], contenenti una serie di raccomandazioni pratiche affinché le organizzazioni possano migliorare la loro posizione di cibersicurezza.

Iniziative legislative

La situazione attuale mette in risalto l'urgenza di **attuare la normativa vigente** e di accelerare l'**adozione delle iniziative in sospeso**.

La Commissione sostiene gli Stati membri nell'attuazione della **direttiva NIS**[11], che impone a questi ultimi di dotarsi di capacità adeguate, istituendo ad esempio un gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) e definendo le autorità competenti. La direttiva fornisce una base per una cooperazione efficace tra gli Stati membri. L'accordo politico raggiunto dai colegislatori sulla **direttiva NIS 2**[12] rappresenta un ulteriore passo avanti nella creazione di un solido quadro dell'UE in materia di preparazione.

NIS 2 – rafforzare ulteriormente la preparazione

- La nuova direttiva sulla sicurezza delle reti e dei sistemi informativi affronterà le carenze della precedente direttiva NIS, adeguandola alle esigenze attuali e future. La direttiva stabilisce norme minime per la definizione di un quadro normativo e istituisce meccanismi per una cooperazione efficace tra le autorità competenti di ciascuno Stato membro.
- La direttiva amplia altresì l'ambito di applicazione delle norme, includendovi nuovi settori critici per l'economia e la società (ad esempio i settori farmaceutico e dei dispositivi medici o il settore della produzione alimentare). Nel suo ambito di applicazione rientreranno tutti i soggetti di medie e grandi dimensioni che operano nei settori interessati o che forniscono servizi contemplati dalla direttiva, nonché gli enti della pubblica amministrazione a livello centrale (esclusi la magistratura, i parlamenti e le banche centrali) e a livello regionale. Gli Stati membri possono inoltre decidere di applicare la direttiva agli enti locali.
- La direttiva NIS 2 definirà lo scenario di base per le misure di gestione dei rischi di cibersicurezza e istituirà formalmente la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), che favorirà la gestione coordinata degli incidenti di cibersicurezza su vasta scala.
- La proposta introduce inoltre disposizioni più precise sulla procedura di segnalazione degli incidenti, sul contenuto delle relazioni e sui termini, e prevede mezzi di ricorso e

8 *Boosting your Organisation's Cyber Resilience* – pubblicazione congiunta, 14.2.2022.
9 Orientamenti sulla sicurezza 2022-01 – *Cybersecurity mitigation measures against critical threats*.
10 Orientamenti di CERT-UE sulla sicurezza 22-002 – *Hardening Signal*.
11 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
12 COM(2020) 823 final.

sanzioni per garantire l'applicazione.
- Gli Stati membri avranno a disposizione 21 mesi a decorrere dall'entrata in vigore della direttiva per recepirne le disposizioni nei rispettivi ordinamenti nazionali.

I progressi compiuti in relazione alla direttiva NIS 2 dovrebbero essere seguiti quanto prima dalla conclusione dei negoziati riguardanti la proposta di **direttiva sulla resilienza dei soggetti critici**[13] ("direttiva CER"), che, una volta adottata e attuata, dovrebbe aumentare la resilienza dei soggetti critici nei confronti di una serie di minacce, tra cui attacchi terroristici, minacce interne o sabotaggio. È inoltre essenziale che il livello di ambizione della direttiva sulla resilienza dei soggetti critici equivalga a quello della proposta della Commissione e che sia mantenuta la coerenza con il compromesso politico raggiunto in relazione alla direttiva NIS 2. Insieme, tali misure rafforzeranno la resilienza e la preparazione istituendo un sistema più coerente e solido, anche mediante piani nazionali di risposta agli incidenti e alle crisi. Le suddette misure erano contemplate anche dalla raccomandazione della Commissione dello scorso anno[14] sull'istituzione dell'**unità congiunta per il ciberspazio**, che delineava come i diversi soggetti coinvolti nell'ecosistema della cibersicurezza (settore diplomatico, delle forze dell'ordine, civile e, se del caso, della difesa) dovessero cooperare a livello operativo. L'attuale panorama delle minacce sottolinea il valore di tale efficace cooperazione tra soggetti essenziali.

La Commissione continua a monitorare l'attuazione del pacchetto di strumenti sulla cibersicurezza del **5G**[15]. In tale contesto, l'11 maggio il gruppo di cooperazione NIS ha adottato una relazione sulla sicurezza di Open RAN[16]. Il gruppo continua inoltre a collaborare con gli Stati membri per rendere pienamente operativo il Centro europeo di competenza per la cibersicurezza.

Il 22 marzo 2022 la Commissione ha proposto **nuove norme per stabilire misure comuni in materia di cibersicurezza e sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'UE**. Tali norme rafforzeranno la resilienza e la capacità dell'amministrazione dell'UE di rispondere alle minacce e agli incidenti informatici. Collocando le suddette attività in un quadro comune, la cooperazione interistituzionale verrà rafforzata e l'esposizione ai rischi verrà ridotta al minimo. La proposta di **regolamento sulla cibersicurezza nelle istituzioni, negli organi e negli organismi dell'UE**[17] rafforzerà il mandato di CERT-UE e porterà alla creazione di un nuovo comitato interistituzionale per la cibersicurezza, consoliderà le capacità in materia di cibersicurezza e incentiverà valutazioni periodiche della maturità e una migliore igiene cibernetica. La proposta di **regolamento sulla sicurezza delle informazioni**[18] creerà una serie minima di norme e standard sulla sicurezza delle informazioni gestite e scambiate da tutte le istituzioni, gli organi e gli organismi dell'UE, in modo da garantire una protezione rafforzata e uniforme contro le mutevoli

[13] COM(2020) 829 final.
[14] Raccomandazione sull'istituzione di un'unità congiunta per il ciberspazio | Plasmare il futuro digitale dell'Europa (europa.eu).
[15] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
[16] Gruppo di cooperazione NIS, *Report on the cybersecurity of Open RAN*, 11 maggio 2022.
[17] COM(2022) 122 final.
[18] COM(2022) 119 final.

minacce nei confronti delle informazioni. La Commissione invita il Parlamento europeo e il Consiglio ad adottare tempestivamente tali misure.

La Commissione ha portato a termine la consultazione pubblica sulle misure volte a rafforzare la **ciberresilienza** dei prodotti digitali e sta attualmente elaborando una proposta che sarà pubblicata in autunno[19]. La proposta farà fronte alle vulnerabilità dei prodotti digitali e dei servizi ausiliari che, pur creando opportunità per le economie e le società dell'UE, comportano anche nuove sfide, dato che più è alto il grado di interconnessione, maggiore è il rischio che un incidente di cibersicurezza si ripercuota su un intero sistema, perturbando così le attività economiche e sociali.

Il 9 marzo 2022 i ministri dell'UE responsabili delle telecomunicazioni hanno adottato all'unanimità l'appello lanciato a Nevers a favore del rafforzamento delle capacità di cibersicurezza dell'Unione, che comprendeva l'attuazione di un nuovo fondo di risposta alle emergenze in materia di cibersicurezza, che sarà istituito dalla Commissione[20]. La Commissione sta riflettendo su come utilizzare al meglio i fondi disponibili per sostenere azioni preventive e di risposta.

Settori critici

La sicurezza dell'approvvigionamento di **energia** dell'UE è fondamentale per il benessere dei cittadini e per il corretto funzionamento delle nostre economie, e la situazione attuale ha messo in evidenza la necessità di stabilire norme chiare in materia di cibersicurezza in questo settore. La Commissione sta lavorando a un codice di rete sulla cibersicurezza per i flussi transfrontalieri di energia elettrica, come previsto dal regolamento sull'energia elettrica[21], al fine di stabilire norme in materia di valutazione dei rischi, requisiti minimi comuni, pianificazione, monitoraggio, comunicazione e gestione delle crisi. Da quando è in corso la guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina, gli obiettivi perseguiti attraverso il codice di rete sulla cibersicurezza sono ancora più pertinenti. La Commissione ha inoltre avviato una cooperazione strutturale tra l'ENISA, l'ENTSO-E[22], l'ENTSO-G[23] e la Comunità dell'energia per quanto riguarda il monitoraggio periodico della situazione della cibersicurezza nel settore dell'energia.

L'UE si è adoperata per salvaguardare la sicurezza dei partner senza creare nuovi rischi per sé stessa. Nel marzo 2022 ha avuto luogo la sincronizzazione di emergenza delle reti elettriche dell'Ucraina e della Moldova con la rete dell'Europa continentale a seguito dell'adozione di misure di attenuazione dei rischi, in particolare per quanto riguarda la cibersicurezza.

La guerra e le sanzioni hanno inoltre comportato numerose sfide per il settore dei **trasporti** dell'UE, dai rischi per la sicurezza dell'aviazione civile e dei conducenti di camion

---

19 Legge sulla ciberresilienza – nuove norme in materia di cibersicurezza per i prodotti digitali e i servizi ausiliari (europa.eu).

20 08/03/2022 – *Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique – Presse – Ministère des Finances* (economie.gouv.fr).

21 Regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sul mercato interno dell'energia elettrica (GU L 158 del 14.6.2019, pag. 54). Una proposta è attualmente all'esame dell'Agenzia per la cooperazione fra i regolatori nazionali dell'energia.

22 Rete europea di gestori di sistemi di trasmissione dell'energia elettrica.

23 Rete europea di gestori del sistema di trasporto del gas.

dell'Unione bloccati nelle zone di conflitto alla distruzione delle infrastrutture di trasporto ucraine, che hanno provocato l'interruzione delle catene di approvvigionamento e messo a rischio la sicurezza dell'approvvigionamento alimentare a livello mondiale. Dall'inizio della guerra l'Agenzia dell'Unione europea per la sicurezza aerea, in stretta collaborazione con la Commissione e con Eurocontrol, l'Organizzazione europea per la sicurezza della navigazione aerea, consiglia agli operatori di non operare all'interno dello spazio aereo dell'Ucraina e di evitare di utilizzare lo spazio aereo entro 100 miglia nautiche dalle frontiere bielorusse e dal confine tra la Russia e l'Ucraina.

La Commissione si adopera inoltre per rafforzare la preparazione e la resilienza del settore dei trasporti dell'UE. In particolare, il 23 maggio è stato adottato un nuovo piano di emergenza per i trasporti[24], che trae insegnamenti sia dalla pandemia di COVID-19 che dall'aggressione militare della Russia nei confronti dell'Ucraina. Il piano propone un pacchetto di 10 azioni che guideranno l'UE e i suoi Stati membri nell'introduzione di misure di risposta alle crisi, garantendo tra l'altro una connettività minima, consolidando la resilienza alle minacce informatiche e ibride e rafforzando la cooperazione con i partner internazionali in materia di preparazione e risposta alle crisi. Viene inoltre sottolineata l'importanza di effettuare test periodici sulla resilienza in diversi scenari di crisi, che coinvolgano tutte le pertinenti agenzie dell'UE o altri soggetti competenti e si basino su processi esistenti.

Nell'ambito del **quadro dell'UE sulla sicurezza sanitaria**, lo scambio di informazioni basato sul sistema di allarme rapido e di reazione, compreso il sostegno agli sgomberi sanitari dall'Ucraina, deve essere protetto dagli attacchi informatici e pertanto la sicurezza del sistema è oggetto di misure di rafforzamento.

Cooperazione con i partner

L'UE continua a collaborare con i suoi partner internazionali per prevenire, scoraggiare e disincentivare i comportamenti dolosi nel ciberspazio e per reagire ad essi. La guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina ha reso la cooperazione in questo settore più importante che mai. A tale riguardo, il SEAE si sta adoperando per condividere la conoscenza situazionale e coordinare la risposta alle attività informatiche dolose che prendono di mira l'Ucraina e si impegna a fornire sostegno all'Ucraina e ad altri soggetti nella regione, collaborando con partner come gli Stati Uniti e la NATO per garantire la complementarità delle azioni ed evitare sovrapposizioni.

La stretta cooperazione con gli Stati Uniti si è intensificata anche nell'ambito del Consiglio UE-USA per il commercio e la tecnologia (TTC). La dichiarazione comune[25] rilasciata a seguito della riunione ministeriale tenutasi a maggio a Parigi ha sottolineato il ruolo centrale del TTC per il partenariato transatlantico rinnovato, che funge da strumento di coordinamento delle misure congiunte intraprese dall'UE e dagli Stati Uniti a fronte dell'aggressione russa nei confronti dell'Ucraina. Entrambe le parti hanno convenuto che una stretta cooperazione volta a promuovere la resilienza delle catene di approvvigionamento è più importante che mai. È stata inoltre istituita una task force dedicata al finanziamento pubblico della sicurezza e della resilienza dell'infrastruttura digitale nei paesi terzi, che aprirà la strada al finanziamento pubblico congiunto USA-UE di progetti digitali nei paesi terzi, sulla base di una serie di principi generali comuni.

[24] COM(2022) 21 final.

[25] https://ec.europa.eu/commission/presscorner/detail/it/STATEMENT_22_3108.

La bussola strategica adottata nel marzo 2022 (cfr. sezione VII) rafforzerà ulteriormente il pacchetto di strumenti della diplomazia informatica dell'UE e favorirà lo sviluppo della politica dell'Unione in materia di ciberdifesa affinché l'UE sia più preparata a rispondere agli attacchi informatici, nell'ambito di una più ampia strategia volta a rafforzare la capacità dell'Unione di intervenire in caso di crisi e difendere i suoi interessi.

Sostegno a favore della cibersicurezza dell'Ucraina e dei paesi vicini

L'UE stava già sostenendo la ciberresilienza dell'Ucraina prima dello scoppio della guerra. Nel giugno 2021 l'UE e l'Ucraina hanno tenuto un primo dialogo in materia di ciberspazio e l'Unione ha fornito sostegno a favore della cibersicurezza e della trasformazione digitale resiliente attraverso il programma EU4Digital Ucraina, del valore di 25 milioni di EUR. È stato inoltre ideato un nuovo programma di gemellaggio del valore di 1,5 milioni di EUR per aiutare le istituzioni ucraine competenti in materia di cibersicurezza ad allinearsi alle norme dell'UE.

A seguito dello scoppio della guerra, l'UE sta promuovendo la cooperazione tra esperti informatici dell'Unione e dell'Ucraina e sta coordinando la fornitura di assistenza tecnica, attrezzature, software e servizi pertinenti per rafforzare la ciberresilienza e la ciberdifesa dell'Ucraina.

L'UE si sta inoltre adoperando per valutare la possibilità di fornire sostegno a medio termine alla Moldova, alla Georgia e ai Balcani occidentali. Il 3 e 4 marzo 2022 è stata effettuata in Moldova una missione congiunta di valutazione delle esigenze in materia di cibersicurezza, che ha portato all'adozione di un'apposita misura di risposta alle crisi volta a incrementare rapidamente la cibersicurezza nel paese. Un analogo sostegno di risposta rapida è in fase di predisposizione per un numero ristretto di paesi dei Balcani occidentali che sono considerati particolarmente a rischio a causa del loro allineamento alle sanzioni dell'UE. L'Unione sta inoltre valutando la possibilità di fornire assistenza supplementare alla Moldova attraverso lo strumento europeo per la pace.

III. CRIMINALITÀ ORGANIZZATA E TERRORISMO

La guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina ha costretto milioni di persone ad abbandonare le proprie case, aumentando notevolmente gli attraversamenti delle frontiere esterne dell'UE. Al 18 maggio erano giunti nell'UE quasi 6 milioni di persone provenienti dall'Ucraina e dalla Moldova e ad oggi 2,8 milioni di queste persone si sono registrati per ottenere protezione temporanea nell'Unione. L'UE ha cercato di fornire accoglienza a quanti fuggono dalla guerra nel modo più rapido e flessibile possibile, senza tuttavia compromettere la sicurezza alle proprie frontiere esterne. L'UE ha adottato misure senza precedenti per offrire alle persone in fuga dalla guerra una protezione temporanea e si è impegnata a gestire tutti i nuovi arrivi senza discriminazioni. Allo stesso tempo, i potenziali rischi derivanti dallo spostamento di un numero così elevato di persone non possono essere trascurati e l'UE, con il solido sostegno delle sue agenzie competenti, continua a vigilare sui nuovi sviluppi riguardanti la criminalità organizzata e il terrorismo.

Uno spazio Schengen forte in un momento di crescenti minacce

Garantire un livello elevato di sicurezza nello spazio **Schengen** e all'interno dell'UE è più importante che mai alla luce delle crescenti minacce derivanti dalla guerra in corso appena oltre le frontiere esterne dell'Unione.

Per realizzare l'ambizioso programma per lo spazio Schengen definito nella strategia del giugno 2021, la Commissione ha adottato a maggio la prima relazione sullo stato di Schengen[26]. Il ciclo annuale di Schengen fornisce un nuovo modello di governance per lo spazio Schengen, prevedendo una verifica periodica dello stato di quest'ultimo. Ciò contribuirà a garantire la rapida individuazione delle carenze e di procedure di follow-up efficienti, così da rendere lo spazio Schengen più forte e più resiliente.

La prima relazione riconosce la necessità di intensificare gli sforzi volti ad attuare iniziative chiave a livello dell'UE, tra cui verifiche sistematiche di tutti i viaggiatori alle frontiere esterne, avvalendosi appieno dei mandati di Frontex ed Europol e degli strumenti proposti e disponibili per la cooperazione transfrontaliera tra le forze di polizia.

In particolare, la nuova architettura e l'interoperabilità dei sistemi di informazione dell'UE per le frontiere, la migrazione e la sicurezza sono la pietra angolare degli sforzi volti a migliorare la sicurezza interna e la gestione delle frontiere. Sarà fondamentale attuare tutti gli elementi del quadro in materia di interoperabilità in modo efficace e nel rispetto delle tempistiche concordate.

Vigilanza e coordinamento

Una maggiore cooperazione tra gli Stati membri e con i paesi terzi in materia di attività di contrasto è fondamentale per garantire la conoscenza delle minacce criminali e terroristiche emergenti e l'azione nei confronti delle reti criminali e degli individui che potrebbero cercare di trarre vantaggio dalla guerra contro l'Ucraina. Gli Stati membri e i partner operativi condividono attivamente le pertinenti informazioni disponibili e l'intelligence criminale con Europol, che effettua controlli incrociati e analisi delle informazioni e le trasforma in notifiche di intelligence operativa utilizzabili, quali notifiche di allarme rapido e valutazioni delle minacce, che sono poi condivise con i partner.

Criminalità organizzata

La criminalità organizzata sta già individuando modi per sfruttare la situazione attuale. L'analisi dell'intelligence preliminare ha individuato in una serie di ambiti fattispecie di reati quali tratta di esseri umani, false dichiarazioni di merci importate ed esportate, frodi online, criminalità informatica e traffico di armi da fuoco. Vi sono inoltre prove del fatto che alcuni criminali informatici fingono di raccogliere fondi per l'Ucraina per rubare denaro e criptovaluta[27]. Le organizzazioni criminali ucraine potrebbero tentare di trasferire le proprie attività a causa della situazione attuale e proseguirle nell'UE.

[26] COM(2022) 301 final.

[27] Il gruppo di analisi delle minacce di Google ha osservato che un numero crescente di autori di minacce utilizza la guerra in Ucraina come esca nelle campagne di phishing e per la diffusione di software maligni. I ricercatori della società Cyren, attiva nel campo della sicurezza su internet, segnalano un aumento delle

La Commissione e la presidenza francese del Consiglio hanno collaborato tra loro, nonché con le agenzie dell'UE che operano nel campo della giustizia e degli affari interni, in particolare Europol, per mobilitare la piattaforma multidisciplinare europea di lotta alle minacce della criminalità (**EMPACT**) allo scopo di valutare, prevedere, prevenire e contrastare le minacce esistenti o emergenti nel settore della criminalità organizzata e delle forme gravi di criminalità. Il 7 aprile 2022 Europol ha ospitato una riunione dell'EMPACT, nell'ambito della quale i rappresentanti e gli esperti degli Stati membri e della comunità della sicurezza dell'UE si sono concentrati sulle minacce nel settore della criminalità organizzata e delle forme gravi di criminalità emerse a seguito della guerra in Ucraina. Tra le misure concrete che sono state oggetto di discussione figurano la raccolta di maggiore intelligence, l'attuazione di misure operative di emergenza e il riorientamento delle misure esistenti, nonché l'organizzazione di giornate di azione congiunta ad hoc.

CELBET (*Customs Eastern and South-Eastern Land Border Expert Team*, gruppo di esperti doganali delle frontiere terrestri orientali e sud-orientali), un progetto di collaborazione finanziato dalla Commissione europea, segue gli sviluppi alla frontiera nell'ambito della sua missione di fornire sostegno operativo e orientamenti ai funzionari doganali e sta monitorando i sequestri doganali presso i valichi alla frontiera tra l'UE (Polonia, Slovacchia, Ungheria e Romania) e l'Ucraina.

Attività criminali e terroristiche

Sebbene nell'UE non sia ancora emersa alcuna minaccia terroristica immediata in relazione all'invasione dell'Ucraina da parte della Russia, è evidente che è necessario vigilare.

I maggiori rischi di attività criminali e terroristiche mettono in risalto l'importanza che gli Stati membri utilizzino le banche dati pertinenti dell'UE, come il sistema d'informazione Schengen, vi inseriscano dati, ove necessario, e le consultino in occasione dei controlli effettuati sulle persone che entrano nell'Unione. Ciò contribuirà a garantire che le persone che rappresentano una minaccia per la sicurezza interna dell'UE siano identificate alle frontiere esterne. L'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) continua a garantire la piena disponibilità ed efficienza dei sistemi di gestione delle frontiere dell'UE. Gli orientamenti[28] forniti agli Stati membri hanno chiarito in che modo bilanciare la necessità di garantire una gestione agevole degli arrivi alle frontiere esterne e l'esecuzione dei necessari controlli di sicurezza.

Preparazione

Oltre all'orientamento e al coordinamento, la preparazione dell'UE è stata rafforzata mediante il dispiegamento di personale delle agenzie dell'Unione.

Europol ha inviato squadre operative negli Stati membri dell'UE confinanti con l'Ucraina. Tali squadre sono composte da agenti di rinforzo di Europol provenienti dagli Stati membri e

truffe riguardanti le criptovalute, che approfittano del conflitto in corso attraverso l'uso di falsi siti web per la raccolta di donazioni.

[28] Comunicazione della Commissione – Orientamenti operativi per la gestione delle frontiere esterne al fine di agevolare l'attraversamento delle frontiere UE-Ucraina (2022/C 104 I/01).

da esperti di Europol in Ungheria, Lituania, Polonia, Romania, Slovacchia e Moldova[29]. Gli agenti di rinforzo di Europol sostengono le autorità nazionali effettuando controlli di sicurezza in seconda linea alle frontiere esterne dell'UE. Gli esperti di Europol forniscono sostegno raccogliendo e valutando informazioni che consentano di individuare minacce terroristiche e criminali, favorire le indagini e identificare persone il cui tentativo di ingresso nell'UE rappresenta un rischio. Le squadre operative raccolgono informazioni che alimentano le valutazioni delle minacce criminali a disposizione degli Stati membri. Tale attività di raccolta di intelligence consente a Europol di prevedere gli sviluppi e coordinare le attività operative con gli Stati membri dell'UE nell'ottica di reagire alle attività dei gruppi criminali che intendono approfittare della guerra in Ucraina e di mettere a frutto la collaborazione attiva instaurata di Europol con le autorità di contrasto ucraine attraverso l'ufficiale di collegamento ucraino presente presso la sede centrale di Europol nei Paesi Bassi.

Anche l'**Agenzia europea della guardia di frontiera e costiera** (**Frontex**) è presente negli Stati membri e nei paesi vicini dell'UE per sostenere le operazioni di controllo delle frontiere: attualmente più di 2 100 guardie di frontiera sono dispiegate in tutta l'UE, nei Balcani occidentali e in Moldova. L'**Ufficio europeo di sostegno per l'asilo** (**EUAA**) ha inviato quasi 750 membri del personale negli Stati membri meridionali dell'UE e in Lituania per sostenere le attività operative, rafforzare le capacità di accoglienza e contribuire alle procedure di asilo.

Sulla base dell'attuale **decisione Prüm**[30], che fornisce un quadro a norma del quale gli Stati membri possono dispiegare funzionari delle autorità di contrasto per lo svolgimento di operazioni congiunte quali pattugliamenti congiunti, la Commissione e la presidenza francese del Consiglio dell'Unione europea hanno inviato una lettera congiunta a tutti gli Stati membri per individuare le esigenze e chiedere il dispiegamento di funzionari di polizia per l'avvio di pattugliamenti congiunti negli Stati membri dell'UE in prima linea che sono maggiormente interessati dai massicci attraversamenti delle frontiere provocati dalla guerra. La Commissione finanzierà tale dispiegamento di forze nell'ambito del Fondo Sicurezza interna – Polizia.

Lotta contro la tratta di esseri umani

Sin dai primi giorni di guerra l'UE vigila sui rischi in una particolare sfera di criminalità che potrebbe trarre vantaggi dai massicci spostamenti di persone in cerca di sicurezza nell'Unione. È infatti essenziale evitare che i trafficanti di esseri umani approfittino della condizione di vulnerabilità delle persone in fuga, che sono per lo più **donne e bambini**, offrendo loro ad esempio finte soluzioni di trasporto o di alloggio.

A marzo Europol ed Eurojust hanno trasmesso alle autorità nazionali competenti notifiche di allarme rapido in merito alla possibilità che persone in fuga dall'Ucraina potessero divenire vittime della tratta di esseri umani e dello sfruttamento. Eurojust contribuisce a migliorare lo scambio di informazioni e ad accelerare la cooperazione giudiziaria, anche con l'Ucraina, e all'agenzia è stato affidato il coordinamento delle indagini sulla tratta di esseri umani.

[29] Al 3 maggio Europol aveva inviato un membro del proprio personale e tre agenti di rinforzo in Slovacchia, un membro del proprio personale in Polonia, un membro del proprio personale e quattro agenti di rinforzo in Romania e due agenti di rinforzo in Ungheria. Un membro del personale di Europol e due agenti di rinforzo sono stati inviati in Moldova.

[30] 2008/615/GAI, 2008/616/GAI.

Il coordinatore anti-tratta dell'UE ha tenuto riunioni con la rete dell'UE dei relatori nazionali e meccanismi equivalenti, con le agenzie che operano nel campo della giustizia e gli affari interni e con la piattaforma della società civile dell'UE contro la tratta di esseri umani, al fine di procedere a uno scambio di informazioni sulle azioni necessarie per prevenire e combattere gli abusi e proteggere le vittime. In diversi Stati membri sono state avviate indagini su potenziali casi.

L'UE è stata rapida e risoluta nel garantire una risposta coordinata a tale minaccia concreta per le persone che necessitano dell'aiuto dell'Unione. Per sostenere le persone in fuga dall'Ucraina sono stati tempestivamente forniti orientamenti operativi[31], anche in merito alla sfida rappresentata dalla tratta di esseri umani, agli Stati membri che attuano la direttiva sulla protezione temporanea. Nell'ambito del piano in 10 punti per rafforzare il coordinamento europeo dell'accoglienza delle persone in fuga dalla guerra in Ucraina[32], presentato al Consiglio "Giustizia e affari interni" il 28 marzo 2022, il coordinatore anti-tratta dell'UE, in collaborazione con le agenzie dell'Unione e gli Stati membri, ha elaborato un piano comune anti-tratta[33] volto a prevenire la tratta di esseri umani e aiutare le vittime. Particolare attenzione è prestata alla registrazione delle entità e delle persone (compresi i volontari) che intendono fornire soluzioni di alloggio e trasporto o altri tipi di assistenza, nonché all'esecuzione di controlli di sicurezza. La Commissione ha inoltre instaurato contatti con l'EUAA per favorire l'individuazione delle vittime della tratta di esseri umani quando nei centri di accoglienza vengono effettuate valutazioni sanitarie. I minori non accompagnati o separati sono particolarmente esposti al rischio di abuso, sfruttamento sessuale o criminalità forzata. I suddetti orientamenti operativi forniscono inoltre indicazioni per aiutare gli Stati membri a gestire l'arrivo, l'accoglienza e il sostegno dei minori, in particolare dei minori non accompagnati. Al fine di sensibilizzare le persone a rischio, la Commissione ha inoltre creato un apposito sito web con una sezione contenente consigli pratici su come evitare i trafficanti.

Sebbene alcune azioni volte a intensificare la preparazione siano state intraprese segnatamente in risposta alle nuove circostanze prodotte dalla guerra, altre misure chiave derivano da **iniziative legislative** già in preparazione prima dello scoppio della guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina.

La Commissione accoglie con favore l'accordo del febbraio 2022 sul mandato riveduto di **Europol**[34], che, quando sarà attuato, consentirà all'agenzia di sostenere meglio gli Stati membri nella lotta contro la criminalità organizzata e il terrorismo. Europol disporrà infatti di strumenti e garanzie adeguati per sostenere le forze di polizia nell'analisi dei *big data* ai fini delle indagini penali e nello sviluppo di metodi pionieristici per contrastare la criminalità informatica. Tali cambiamenti saranno accompagnati da un quadro rafforzato per la protezione dei dati e dal consolidamento del controllo parlamentare e dell'obbligo di rendicontabilità.

[31] C/2022/1806, EUR-Lex - 52022XC0321(03) - IT - EUR-Lex (europa.eu).
[32] https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_it.
[33] https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_it.
[34] COM(2020) 796 final.

Il pacchetto sulla **cooperazione di polizia**, presentato dalla Commissione l'8 dicembre 2021[35] e attualmente oggetto di negoziati, rafforzerà la cooperazione tra i funzionari delle autorità di contrasto in tutti gli Stati membri, rendendo lo scambio di dati più rapido, più semplice e più sicuro, nonché potenziando e rendendo più efficiente la cooperazione operativa di polizia sul campo. La Commissione invita il Parlamento europeo e il Consiglio ad adottare rapidamente il pacchetto.

Una volta adottate e attuate, le suddette proposte legislative favoriranno le attività di contrasto della criminalità organizzata transfrontaliera. Ciò sarà particolarmente importante in un contesto in cui le organizzazioni criminali ucraine potrebbero tentare di trasferire le proprie attività a causa della situazione attuale e proseguirle nell'UE.

La **missione consultiva dell'UE in Ucraina** sostiene sin dal 2014 la riforma delle istituzioni preposte all'applicazione della legge e dello Stato di diritto nel paese. Nel marzo 2022 il mandato della missione è stato riveduto per consentirle di fornire sostegno presso i valichi di frontiera ucraini con Polonia, Romania e Slovacchia e contribuire alla conoscenza situazionale delle attività criminali transfrontaliere, compresa la tratta di esseri umani, e del flusso di approvvigionamenti umanitari verso l'Ucraina.

IV. ARMI, MATERIALI PERICOLOSI E INCIDENTI CRITICI

La guerra ha aumentato massicciamente la circolazione di armi da fuoco e di altri tipi di armi all'interno dell'Ucraina, determinando nuovi rischi per l'UE e per gli altri Stati confinanti con l'Ucraina.

Vigilanza e coordinamento

Gli orientamenti operativi pubblicati a marzo hanno fornito agli Stati membri indicazioni su come affrontare la sfida dell'aumento della circolazione di armi da fuoco in un momento in cui si registrano massicci afflussi di persone alle frontiere esterne dell'UE[36]. Gli orientamenti sottolineano che la presenza di armi da fuoco dovrebbe essere sottoposta a controllo costante e che nessuno dovrebbe poter entrare nell'UE con un'arma da fuoco senza autorizzazione. Ove le autorità ucraine dovessero segnalare la sparizione di un'arma da fuoco, gli Stati membri dovrebbero inserire una segnalazione nel sistema d'informazione Schengen.

È essenziale che tutte le spedizioni di armi da fuoco verso l'Ucraina siano registrate correttamente, indicando tutte le informazioni pertinenti (compresi tipo, paese e anno di fabbricazione, marchio, marca, calibro, numero di serie) al fine di agevolare la tracciabilità delle armi, sia in Ucraina che nell'UE.

L'UE ha condannato pubblicamente gli sconsiderati attacchi militari della Russia ai danni di impianti chimici, biologici e nucleari civili in Ucraina e nelle loro immediate vicinanze, nonché qualsiasi atto che comprometta la sicurezza di tali impianti. La Commissione monitora la situazione in Ucraina, prestando particolare attenzione alla minaccia radiologica, che desta la massima preoccupazione dal punto di vista della sicurezza interna dell'UE[37]. La

[35] COM(2021) 780 final, COM(2021) 782 final e COM(2021) 784 final.

[36] Comunicazione della Commissione – Orientamenti operativi per la gestione delle frontiere esterne al fine di agevolare l'attraversamento delle frontiere UE-Ucraina (2022/C 104 I/01).

[37] La Commissione organizzerà, in collaborazione con i partner statunitensi, un seminario incentrato sui rischi connessi ai materiali radiologici situati negli ospedali che sfuggono al controllo regolamentare.

Commissione monitora inoltre le potenziali minacce chimiche e ha istituito un meccanismo di coordinamento interno nel caso in cui sia necessaria una rapida valutazione del rischio.

Preparazione

L'Ucraina è già uno dei paesi ritenuti fondamentali per azioni specifiche a livello esterno nell'ambito del piano d'azione dell'UE sul traffico di armi da fuoco 2020-2025. Nell'ambito della componente dell'EMPACT dedicata alle armi da fuoco è inoltre prevista un'azione operativa specifica nella regione che comprende l'Ucraina. Tuttavia, alla luce dei rischi di sviamento delle armi da fuoco, saranno necessari progetti specifici finanziati dall'UE nonché una cooperazione operativa con Europol, Frontex e la componente dell'EMPACT dedicata alle armi da fuoco. La Commissione presenterà a breve una proposta di revisione del regolamento sulle armi da fuoco [38] per quanto riguarda le esportazioni, le importazioni e il transito di armi da fuoco ad uso civile, nell'ambito del quadro giuridico e operativo generale finalizzato alla prevenzione, all'accertamento, all'indagine e all'esercizio dell'azione penale nei confronti della tratta di esseri umani.

Per migliorare la preparazione e la risposta dell'UE ai rischi per la salute pubblica come le minacce chimiche, biologiche, radiologiche e nucleari (CBRN), la Commissione sta costituendo riserve strategiche di capacità di risposta attraverso il meccanismo unionale di protezione civile (UCPM), con il finanziamento dall'Autorità europea per la preparazione e la risposta alle emergenze sanitarie (HERA)[39]. I servizi della Commissione stanno collaborando alla creazione di una scorta strategica rescEU del valore di 540,5 milioni di EUR. La scorta comprenderà attrezzature e medicine, vaccini e altri trattamenti che consentano di curare pazienti esposti ad agenti CBRN in emergenza, come pure una riserva di decontaminazione rescEU composta da attrezzature di decontaminazione ed équipe di risposta specializzate. Come primo passo immediato, l'UE ha mobilitato la sua riserva medica rescEU per l'approvvigionamento di compresse di ioduro di potassio, che possono essere utilizzate per proteggere le persone dagli effetti nocivi delle radiazioni, e altri prodotti urgentemente necessari in Ucraina. Quasi 3 milioni di compresse di ioduro sono già state consegnate all'Ucraina attraverso l'UCPM, con l'aiuto di Francia e Spagna.

V. AZIONE COORDINATA PER CHIAMARE LA RUSSIA A RISPONDERE DELL'AGGRESSIONE

L'UE sta svolgendo un ruolo decisivo nelle azioni intraprese dalla comunità internazionale per esercitare pressioni sulla Russia affinché ponga fine alla sua aggressione nei confronti dello Stato ucraino e dei civili coinvolti nel conflitto, che è inaccettabile e contraria al diritto internazionale. Tali azioni comprendono misure volte a definire le conseguenze per i responsabili, comprese severe sanzioni, e azioni volte ad accertare i crimini di guerra commessi e agevolare l'esercizio dell'azione penale.

[38] Regolamento (UE) n. 258/2012 del Parlamento europeo e del Consiglio, del 14 marzo 2012, che attua l'articolo 10 del protocollo delle Nazioni Unite contro la fabbricazione e il traffico illeciti di armi da fuoco, loro parti e componenti e munizioni, addizionale alla convenzione delle Nazioni Unite contro la criminalità transnazionale organizzata (protocollo delle Nazioni Unite sulle armi da fuoco), e dispone autorizzazioni all'esportazione, misure di importazione e transito per le armi da fuoco, loro parti e componenti e munizioni.

[39] Piano di lavoro dell'HERA per il 2022 (europa.eu).

Misure restrittive e confisca

Da quando la Russia ha concesso il proprio riconoscimento alle zone degli oblast di Donetsk e Luhansk non controllate dal governo ucraino il 21 febbraio 2022 e ha invaso l'Ucraina il 24 febbraio 2022, l'UE ha inflitto alla Russia la più ampia serie di misure restrittive mai adottate. Sinora sono stati adottati cinque pacchetti di sanzioni. Tali misure si concentrano su settori chiave, tra cui finanza, commercio, trasporti, difesa e mezzi di informazione, e sono dirette nei confronti delle élite politiche e militari e degli oligarchi russi e bielorussi di spicco. Gli elenchi comprendono già oltre 1 000 persone e 80 entità. Il Consiglio sta attualmente discutendo un sesto pacchetto di sanzioni.

La forza dell'impatto delle attuali e delle precedenti misure restrittive nei confronti di società e cittadini russi e bielorussi dipenderà dalla rigorosità della loro applicazione. Il coordinamento dell'UE può contribuire in misura notevole a colmare potenziali lacune e la Commissione ha fornito ampio sostegno ai portatori di interessi elaborando orientamenti scritti, organizzando riunioni dei portatori di interessi, istituendo un apposito gruppo di esperti e mettendo a disposizione una serie di risorse per agevolare il rispetto delle misure.

La Commissione ha inoltre istituito la task force "Freeze and Seize", che riunisce i servizi della Commissione, gli Stati membri, Eurojust ed Europol. Sinora gli Stati membri hanno dichiarato di aver sottoposto a congelamento beni per un valore di 9,89 miliardi di EUR[40]. L'11 aprile Europol, insieme agli Stati membri, a Eurojust e a Frontex, ha avviato l'operazione Oscar per favorire le indagini finanziarie e penali riguardanti beni derivanti da attività criminali detenuti da persone fisiche e giuridiche oggetto di sanzioni dell'UE connesse alla guerra intrapresa dalla Russia nei confronti dell'Ucraina. La task force "Freeze and Seize" dell'UE lavora a stretto contatto con la task force "Russian Elites, Proxies and Oligarchs" (REPO), istituita dai paesi del G7 (Canada, Francia, Germania, Italia, Giappone, Regno Unito, Stati Uniti) e da partner che condividono gli stessi principi, come l'Australia, nonché con la task force statunitense KleptoCapture e con la task force ucraina.

La task force "Freeze and Seize" funge da piattaforma per coordinare e agevolare lo scambio di informazioni ed esperienze tra gli Stati membri, fornire orientamenti sull'attuazione delle sanzioni e facilitare lo scambio di migliori pratiche in materia di indagini penali e confisca. In particolare, è importante che le autorità di contrasto siano vigili e proattive in relazione a potenziali reati ad opera delle persone ed entità sanzionate. La task force mira inoltre a favorire le discussioni sull'eventuale impiego delle risorse confiscate, ad esempio per contribuire alla ricostruzione dell'Ucraina.

La Commissione adotta oggi un pacchetto sul **recupero e sulla confisca dei beni**[41] che tiene conto degli insegnamenti tratti dall'attuazione delle misure restrittive dell'Unione nei confronti di persone ed entità russe e bielorusse. Il pacchetto agevolerà l'efficace attuazione delle misure restrittive dell'Unione in tutta l'UE, consentendo di reperire e identificare rapidamente i beni di proprietà o sotto il controllo di persone o entità soggette a tali misure. Il quadro rafforzato in materia di recupero e confisca dei beni si applicherà anche alla violazione delle misure restrittive e garantirà in tal modo l'efficace reperimento, congelamento, gestione e confisca dei proventi derivanti dalla violazione di tali misure. Per garantire che i beni delle persone e delle entità che violano le misure restrittive possano

[40] Sono inoltre stati bloccati attivi della Banca centrale russa pari a circa 23 miliardi di EUR.
[41] COM(2022) 245 final.

essere effettivamente confiscati, la Commissione adotta oggi anche proposte di decisione del Consiglio volte ad aggiungere la violazione delle sanzioni all'elenco dei reati dell'UE di cui all'articolo 83, paragrafo 1, TFUE[42], accompagnate da una comunicazione[43], nell'ottica di proporre una direttiva volta a ravvicinare la definizione dei reati e delle sanzioni per le violazioni delle misure restrittive.

In generale, il pacchetto rappresenta un passo fondamentale nella lotta contro la criminalità organizzata, dando seguito agli impegni assunti dalla Commissione nella strategia per l'Unione della sicurezza e nella strategia per la lotta alla criminalità organizzata 2020-2025[44]. Il pacchetto effettua una revisione della direttiva del 2014 relativa alla confisca, della decisione del Consiglio del 2007 relativa agli uffici per il recupero dei beni e della decisione quadro del 2005 relativa alla confisca di beni, strumenti e proventi di reato, nell'ottica di rafforzare le capacità di reperimento e identificazione e, in ultima analisi, di confisca dei proventi illeciti, facendo fronte ai bassissimi tassi di confisca nell'UE[45]. Il pacchetto amplia la portata dei reati contemplati ed estende le norme sulla confisca nei casi in cui una condanna penale per un reato specifico non sia possibile, ma i beni derivino chiaramente da attività criminali. La revisione rafforza inoltre la gestione efficace dei beni sottoposti a congelamento e a confisca e consolida la capacità degli uffici per il recupero dei beni di reperire e identificare beni illeciti. Il nuovo quadro dell'UE in materia di recupero dei beni è concepito per far fronte al complesso modus operandi delle organizzazioni criminali, che spesso operano a livello transfrontaliero e utilizzano diversi metodi per occultare i loro beni, ricorrendo anche alle cripto-attività.

Risposta giudiziaria coordinata

Sono inoltre in corso attività a livello dell'UE per garantire una risposta giudiziaria coordinata ai presunti **crimini internazionali** commessi in Ucraina, affinché i responsabili possano essere chiamati a rispondere delle loro azioni.

Due Stati membri e l'Ucraina hanno istituito una squadra investigativa comune per indagare sui crimini di guerra, sui crimini contro l'umanità e su altri crimini internazionali presumibilmente commessi sul territorio ucraino. La squadra riceve sostegno giuridico, analitico, finanziario e logistico da Eurojust. Il 25 aprile 2022 l'ufficio del procuratore della Corte penale internazionale si è unito alla squadra in qualità di partecipante[46] e si prevede che altri soggetti entreranno a farne parte a breve.

Il 25 aprile 2022 la Commissione ha presentato una proposta di modifica del regolamento Eurojust[47] affinché l'agenzia preservi, analizzi e conservi le prove dei principali reati internazionali. Eurojust ed Europol continueranno a collaborare strettamente nel corso dell'intero processo. Un ruolo cruciale nel coordinamento della risposta giudiziaria è svolto anche dalla rete sul genocidio, di cui Eurojust ospita il segretariato, che ha preparato un

[42] COM(2022) 247 final.
[43] COM(2022) 249 final.
[44] COM(2021) 170 final.
[45] Secondo le stime di Europol, solo il 2 % dei beni derivanti da attività criminali è sottoposto a congelamento (2,4 miliardi di EUR) e solo l'1 % è confiscato (1,2 miliardi di EUR), mentre i proventi della criminalità nei principali mercati criminali dell'UE ammontavano a 139 miliardi di EUR nel 2019 (pari all'1 % del PIL dell'UE).
[46] https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine.
[47] COM(2022) 187 final.

atlante delle ONG attualmente attive in Ucraina e che sostiene gli operatori nazionali degli Stati membri e dell'Ucraina che si occupano di casi aperti connessi alla guerra.

Nell'aprile 2022 il Consiglio ha ulteriormente riveduto il mandato della **missione consultiva dell'UE in Ucraina**, consentendole di fornire sostegno alle autorità ucraine nelle indagini e nel perseguimento di eventuali crimini internazionali commessi nel contesto dell'aggressione militare russa. La missione fornirà alle autorità ucraine consulenza strategica sullo svolgimento delle indagini e sul perseguimento dei crimini internazionali, sulle necessarie modifiche della legislazione ucraina, sulla strategia di comunicazione e sulla formazione riguardante questioni correlate. La missione è parte integrante di una serie di pertinenti iniziative di coordinamento e, insieme alla delegazione dell'UE, fa parte del gruppo consultivo USA-UE per l'Ucraina sui crimini atroci.

VI. MANIPOLAZIONE DELLE INFORMAZIONI E INGERENZA DA PARTE DI SOGGETTI STRANIERI

Gli attuali sviluppi geopolitici hanno messo in evidenza i rischi di ingerenze straniere. L'aggressione militare russa nei confronti dell'Ucraina è accompagnata da attività di **manipolazione delle informazioni e ingerenza**. Per giustificare i brutali attacchi ai danni dell'Ucraina sono state utilizzate accuse immotivate di "nazismo" e "genocidio" nei confronti del governo ucraino, operazioni sotto falsa bandiera e accuse infondate nei confronti della NATO e dell'Occidente, mentre la libertà di parola e l'informazione indipendente all'interno della Russia sono state soppresse. Permane il rischio che la Russia possa tentare di utilizzare materiali audiovisivi manipolati e la disinformazione come pretesto per sferrare ulteriori attacchi militari, indebolire la determinazione della resistenza ucraina, dividere la comunità internazionale nella sua opposizione alla guerra o destare dubbi sulle violazioni del diritto internazionale da parte della Russia. Nell'ambito della bussola strategica, l'UE si è impegnata a reagire con fermezza alla manipolazione delle informazioni e all'ingerenza da parte di soggetti stranieri, nonché a rafforzare la propria resilienza e capacità di contrastare tali minacce[48]. La manipolazione del dibattito democratico all'interno dell'UE è oggetto del piano d'azione per la democrazia europea, il piano coordinato della Commissione per contrastare la disinformazione e rafforzare la resilienza democratica[49].

Vigilanza e coordinamento

L'Unione europea ha reagito con un'azione risoluta e coordinata alla campagna di disinformazione intrapresa dalla Russia nel contesto dell'aggressione militare nei confronti dell'Ucraina. L'UE ha collaborato strettamente con i propri Stati membri attraverso il sistema di allarme rapido e con partner internazionali quali la NATO, gli Stati Uniti, il Canada e il meccanismo di risposta rapida del G7 per condividere le conoscenze sulle tendenze e le tattiche di manipolazione del Cremlino. Sono state intensificate le attività volte a smontare le manipolazioni del Cremlino, in particolare attraverso il sito web EUvsDisinfo, che diffonde all'interno dell'UE, dell'Ucraina e della regione, nonché all'interno della Russia, informazioni basate sui fatti in inglese, russo, ucraino e in altre lingue. Dal 2 marzo le trasmissioni dei media di Stato russi RT e Sputnik nell'UE o verso l'UE sono sospese a seguito delle misure restrittive adottate dall'Unione. Le piattaforme online, i principali social network, gli inserzionisti e i soggetti dell'industria pubblicitaria che hanno sottoscritto il codice di buone

[48] https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/it/pdf.
[49] COM(2020) 790 final.

pratiche sulla disinformazione[50] stanno adottando misure urgenti per arginare la disinformazione legata all'aggressione russa nei confronti dell'Ucraina. La Commissione e il SEAE monitorano tali sforzi. Le informazioni fornite mostrano che le piattaforme hanno rafforzato i loro strumenti di monitoraggio e di intervento in relazione alla guerra.

Inoltre si stanno rapidamente varando azioni per aiutare i paesi dell'Asia centrale e dei Balcani occidentali a rafforzare la resilienza dell'informazione e contrastare la manipolazione delle informazioni e la disinformazione ad opera di soggetti stranieri.

Preparazione

L'evidente ricorso alla manipolazione delle informazioni e all'ingerenza da parte di soggetti stranieri, compreso l'utilizzo della disinformazione come strumento di minaccia ibrida, ha reso ancora più urgente l'esigenza di dare seguito al piano d'azione per la democrazia europea. Negli ultimi mesi le istituzioni dell'UE hanno sostenuto gli Stati membri nella lotta contro la manipolazione delle informazioni e l'ingerenza da parte di soggetti stranieri, in particolare nel quadro del sistema di allarme rapido, condividendo informazioni sulle tattiche utilizzate dai soggetti responsabili e sulle strategie di risposta. Sono attualmente in corso discussioni sull'ulteriore rafforzamento della risposta globale dell'UE alla manipolazione delle informazioni e all'ingerenza da parte di soggetti stranieri, sulla base di un documento di riflessione presentato dal SEAE sullo sviluppo di un apposito **pacchetto di strumenti** per affrontare la minaccia in questione. Il pacchetto riunirà le misure interne esistenti e i nuovi strumenti dell'UE nell'ambito della politica estera e di sicurezza comune e trarrà benefici dall'intensificazione dell'azione della divisione StratCom del Servizio europeo per l'azione esterna[51] e della Commissione.

L'Osservatorio europeo dei media digitali (EDMO) ha istituito una task force sulla disinformazione a seguito dello scoppio della guerra in Ucraina e coordina le azioni dei verificatori dei fatti e dei ricercatori nella sua rete. Esso ha analizzato il modo in cui i fautori dell'idea che dietro la COVID-19 si celasse un complotto si sono rapidamente trasformati in propugnatori di notizie false di matrice filorussa, una tendenza osservata in vari Stati membri[52].

La proposta di legge sui servizi digitali intende far sì che la normativa sia al passo con la rapida evoluzione delle tecnologie digitali e con le sfide tecnologiche e democratiche correlate, quali l'incitamento all'odio, la disinformazione online e le strategie di destabilizzazione. I significativi progressi compiuti nell'ambito dei negoziati avviati dal Parlamento europeo e dal Consiglio dovrebbero consentire una tempestiva adozione del pacchetto.

---

[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[51] La divisione Comunicazione strategica, task force e analisi delle informazioni del Servizio europeo per l'azione esterna fornisce sostegno strategico in materia di comunicazione nell'attuazione della politica estera e di sicurezza dell'UE nelle relative regioni prioritarie (vicinato meridionale e orientale, Balcani occidentali), sviluppando e attuando specifiche azioni di comunicazione strategica incentrate sulla promozione delle politiche, dei valori, degli obiettivi e degli interessi dell'Unione.

[52] https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/.

VII. PREPARAZIONE GENERALE

In un'epoca in cui la guerra si è riaffacciata sul territorio europeo, nonché in un periodo di grandi mutamenti geopolitici, il coordinamento della sicurezza nell'UE si è intensificato, facendo leva su iniziative già in preparazione prima dello scoppio della guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina. Le iniziative incentrate principalmente sulla sicurezza esterna dell'UE hanno considerevoli implicazioni per l'agenda interna riguardante l'Unione della sicurezza.

Il 15 febbraio 2022 la Commissione ha presentato il **pacchetto difesa**[53], recante una serie di iniziative in settori critici per la difesa e la sicurezza all'interno dell'UE. Il contributo della Commissione alla difesa e alla sicurezza europee affronta l'intera gamma delle sfide attuali, propone misure concrete per rendere più integrato e competitivo il mercato europeo della difesa, rafforzando in particolare la cooperazione all'interno dell'UE e realizzando economie di scala, e delinea una tabella di marcia per promuovere la ricerca, lo sviluppo tecnologico e l'innovazione nei settori delle tecnologie critiche per la sicurezza e la difesa e ridurre le dipendenze di tali tecnologie e delle catene del valore. Il pacchetto mira inoltre a rafforzare la dimensione della politica spaziale dell'UE legata alla difesa ed esamina in che modo la Commissione potrebbe consolidare la propria azione di contrasto delle minacce ibride, anche nel settore informatico, migliorare la mobilità militare all'interno e al di fuori dell'Europa e affrontare ulteriormente le sfide in materia di cambiamenti climatici legate alla difesa. A integrazione di questo lavoro, la comunicazione congiunta del 18 maggio **sull'analisi delle carenze di investimenti nel settore della difesa e sulle prospettive di percorso**[54] prende in esame le lacune industriali e di capacità da colmare per sostenere gli Stati membri dell'UE maggiormente esposti e individuare misure in grado di attenuare le carenze individuate.

La resilienza dell'UE a tali minacce implica anche approcci basati sulle capacità in tutti i settori della sicurezza, come ribadito nel piano d'azione della Commissione sulle sinergie tra l'industria civile, della difesa e dello spazio[55]. Sono in corso attività volte a promuovere approcci basati sulle capacità nel settore della sicurezza interna e dell'applicazione della legge.

Il 21 marzo 2022 il Consiglio ha adottato la **bussola strategica per la sicurezza e la difesa**[56], che è stata approvata poco dopo dal Consiglio europeo. La bussola delinea un ambizioso piano d'azione per rafforzare la politica di sicurezza e di difesa dell'UE entro il 2030. L'obiettivo è rendere l'UE un garante della sicurezza più forte e capace, in grado di proteggere i suoi cittadini e contribuire alla pace e alla sicurezza internazionali. La bussola contiene proposte concrete, corredate di un calendario di attuazione molto preciso, allo scopo di migliorare la capacità dell'UE di agire con decisione durante le crisi.

Uno dei risultati che la bussola strategica si prefigge di raggiungere è lo sviluppo di un **pacchetto di strumenti dell'UE contro le minacce ibride**, che dovrebbe fornire un quadro per una risposta coordinata alle campagne ibride che interessano l'Unione e i suoi Stati

---

53 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_it.

54 JOIN(2022) 24 final.

55 COM(2021) 70 final.

56 Una bussola strategica per la sicurezza e la difesa – Per un'Unione europea che protegge i suoi cittadini, i suoi valori e i suoi interessi e contribuisce alla pace e alla sicurezza internazionali: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/it/pdf.

membri, comprese misure interne ed esterne. A seguito dell'individuazione di parametri di riferimento settoriali per la resilienza, effettuata all'inizio del 2022[57], verrà eseguita un'analisi delle carenze e delle esigenze. È in tale contesto che l'UE continuerà a consolidare la preparazione, la resilienza e la risposta alle minacce derivanti dall'aggressione russa e da qualsiasi altro tentativo di destabilizzare le democrazie e il multilateralismo basato su regole.

VIII. GUARDANDO AL FUTURO

Guardando al futuro, l'UE dovrà rimanere estremamente vigile nei confronti dell'evoluzione delle minacce e consolidare **la preparazione e la resilienza a tutte le eventualità**. Le ripercussioni della guerra possono assumere forme diverse, non tutte attualmente valutabili.

L'entità del trasferimento delle attività delle reti criminali ucraine all'estero non è ancora nota. L'attività operativa svolta da Eurojust in passato indica che il traffico di eroina diretto dall'Afghanistan verso l'UE passa tendenzialmente attraverso l'Ucraina, come confermato dall'Osservatorio europeo delle droghe e delle tossicodipendenze (EMCDDA)[58]. L'instabilità potrebbe rendere più difficile contrastare il traffico di eroina lungo questa rotta, con il rischio che il flusso di stupefacenti verso l'UE possa aumentare.

Alcuni rischi per l'UE hanno maggiori probabilità di aumentare al termine o durante potenziali sospensioni delle ostilità. Verrà prestata particolare attenzione alla circolazione delle armi da fuoco, che rischia di aumentare quando i combattimenti in Ucraina si placheranno. Le esperienze passate mettono inoltre in evidenza il rischio che il ritorno in patria di combattenti stranieri che hanno acquisito esperienza nei combattimenti e che potrebbero essere entrati in contatto con gruppi estremisti possa comportare l'avvio di attività terroristiche nell'UE in una fase successiva. Questo potenziale fenomeno dovrebbe essere attentamente monitorato e la Commissione sta già favorendo discussioni tra gli Stati membri in merito alle sfide poste dal ritorno in patria di volontari stranieri con un passato legato all'estremismo violento.

Alla luce di tali possibili minacce, è importante portare avanti l'attuazione della strategia per l'Unione della sicurezza, anche con l'attuazione di strategie chiave quali la strategia dell'UE in materia di cibersicurezza, la strategia per la lotta alla criminalità organizzata (2020-2025), il programma di lotta al terrorismo dell'UE (2020-2025), il piano d'azione dell'UE sul traffico di armi da fuoco (2020-2025), la strategia dell'UE per la lotta alla tratta degli esseri umani (2021-2025) e la strategia dell'UE in materia di droghe (2021-2025).

Proseguiranno gli sforzi volti a dotare l'UE del necessario quadro legislativo. Ad esempio, la Commissione sta preparando la valutazione d'impatto per una proposta che disciplini la commercializzazione e l'uso di sostanze chimiche ad alto rischio.

---

[57] SWD(2022) 21 final.

[58] *Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data)*, EMCDDA, *Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery*, 2021/00446, Eurojust, maggio 2020.

IX. CONCLUSIONI

L'Unione della sicurezza continua a svolgere il proprio ruolo nel preparare l'UE e i suoi Stati membri ad affrontare le minacce esistenti e potenziali. La guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina ha messo in luce la velocità con cui le minacce teoriche possano concretizzarsi e sottolinea l'importanza della vigilanza, del coordinamento e della preparazione.

Questa quarta relazione sui progressi compiuti nella strategia dell'UE per l'Unione della sicurezza dimostra che l'UE è in grado di adattarsi, anche a fronte di minacce eccezionali e impreviste come la guerra di aggressione intrapresa dalla Russia nei confronti dell'Ucraina. Attuare con determinazione la strategia per l'Unione della sicurezza è più importante che mai.