COMMISSIONE
EUROPEA

ALTO RAPPRESENTANTE
DELL'UNIONE PER
GLI AFFARI ESTERI E
LA POLITICA DI SICUREZZA

Bruxelles, 19.7.2017
JOIN(2017) 30 final

RELAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO

sull'attuazione del Quadro congiunto per contrastare le minacce ibride – La risposta dell'Unione europea

1. INTRODUZIONE

L'UE sta affrontando una delle più grandi sfide alla sicurezza della sua storia. Le minacce assumono sempre più fattezze non convenzionali: da quelle fisiche, come le nuove forme di terrorismo, a quelle che utilizzano lo spazio digitale per sferrare complessi attacchi informatici. Altre sono più sottili e mirano a esercitare una pressione coercitiva, come le campagne di disinformazione e la manipolazione dei media, che si propongono di mettere a repentaglio valori europei fondamentali quali la dignità umana, la libertà e la democrazia. I recenti attacchi informatici sferrati in maniera coordinata in tutto il mondo, per i quali è stato difficile risalire a un colpevole, hanno evidenziato le vulnerabilità delle nostre società e istituzioni.

Nell'aprile 2016 la Commissione europea e l'Alto rappresentante hanno adottato una comunicazione congiunta su un Quadro congiunto per contrastare le minacce ibride[1]. Riconoscendo la natura complessa e transfrontaliera delle minacce ibride, il Quadro propone un approccio esteso a tutti i livelli dell'amministrazione per rafforzare la resilienza globale delle nostre società. Il Consiglio[2] ha accolto con favore l'iniziativa e le azioni proposte, e invitato la Commissione e l'Alto rappresentante a presentare una relazione sui progressi compiuti nel luglio 2017. Sebbene l'UE possa assistere gli Stati membri nel consolidamento della loro resilienza nei confronti delle minacce ibride, la responsabilità principale ricade sugli Stati membri, nella misura in cui la lotta contro le minacce ibride attiene alla difesa e alla sicurezza nazionale.

Il Quadro congiunto per contrastare le minacce ibride costituisce un elemento importante dell'approccio globale più integrato dell'UE alla sicurezza e alla difesa. Contribuisce alla creazione di "un'Europa che protegge", evocata dal presidente Juncker nel discorso sullo stato dell'Unione del settembre 2016. Nel 2016 l'Unione europea ha inoltre posto le basi per un rafforzamento della politica di difesa europea al fine di rispondere alle aspettative di maggiore protezione dei cittadini. La strategia globale dell'UE in materia di politica estera e di sicurezza[3] ha illustrato in dettaglio la necessità di un approccio integrato che coniughi resilienza interna e azioni esterne dell'UE, nonché di sinergie tra la politica di difesa e le politiche riguardanti il mercato interno, l'industria, l'applicazione della legge e i servizi di intelligence. A seguito dell'adozione, nel novembre 2016, del piano di azione europeo in materia di difesa, la Commissione ha presentato iniziative concrete che contribuiranno a rafforzare la capacità dell'UE di rispondere alle minacce ibride incrementando la resilienza delle catene di approvvigionamento europee nel settore della difesa e consolidando il mercato unico per la difesa. In particolare, il 7 giugno 2017 la Commissione ha varato il Fondo europeo per la difesa, con finanziamenti proposti per 600 milioni di euro fino al 2020 e 1,5 miliardi di euro all'anno dopo il 2020. La comunicazione relativa all'Unione della sicurezza[4] ha riconosciuto la necessità di contrastare le minacce ibride e l'importanza di garantire maggiore coerenza tra le azioni interne ed esterne nel settore della sicurezza.

[1] Comunicazione congiunta al Parlamento europeo e al Consiglio *Quadro congiunto per contrastare le minacce ibride – La risposta dell'Unione europea*, JOIN(2016) 18 final.
[2] *Conclusioni del Consiglio sul contrasto alle minacce ibride*, comunicato stampa 196/16 del 19 aprile 2016.
[3] Presentata dall'Alto rappresentante al Consiglio europeo il 28 giugno 2016.
[4] COM(2016) 230 final del 20.4.2016.

I leader dell'UE hanno collocato la sicurezza e la difesa al centro del dibattito sul futuro dell'Europa[5], come riconosciuto nella dichiarazione di Roma, del 25 marzo 2017, che evoca l'idea di un'Unione sicura e impegnata a rafforzare la sicurezza e la difesa comuni. L'8 luglio 2016 i presidenti del Consiglio europeo e della Commissione europea e il segretario generale della NATO hanno sottoscritto a Varsavia una dichiarazione congiunta con l'obiettivo di imprimere un nuovo impulso al partenariato strategico UE-NATO e concretizzarlo ulteriormente. La dichiarazione congiunta ha evidenziato sette aree concrete nelle quali la cooperazione tra le due organizzazioni dovrebbe essere potenziata, compresa la lotta contro le minacce ibride. Successivamente i ministri dell'UE e della NATO hanno approvato un insieme comune di 42 proposte di attuazione e nel giugno 2017 è stata pubblicata una prima relazione, in cui sono evidenziati i significativi progressi compiuti[6].

Il documento di riflessione della Commissione sul futuro della difesa europea[7], presentato nel giugno 2017, delinea diversi scenari in merito alle modalità per rispondere alle crescenti minacce cui deve far fronte l'Europa nel campo della sicurezza e della difesa e per accrescere la capacità di difesa dell'Europa entro il 2025. In tutti e tre gli scenari la sicurezza e la difesa sono considerate parte integrante del progetto europeo al fine di proteggere e promuovere i nostri interessi tanto all'interno quanto all'esterno. L'Europa deve diventare un garante della sicurezza e assicurare progressivamente la sua stessa sicurezza. Nessuno Stato membro può affrontare da solo le sfide future, in particolare quella della lotta contro le minacce ibride. La cooperazione in materia di difesa e sicurezza non è pertanto una possibilità, ma una necessità, per un'Europa davvero in grado di proteggere.

La presente relazione mira a riferire sui progressi compiuti e sulle prossime fasi di attuazione in merito alle azioni nelle quattro aree proposte dal Quadro congiunto: migliorare la consapevolezza situazionale, rafforzare la resilienza, rafforzare le capacità degli Stati membri e dell'Unione di prevenire le crisi, reagirvi e riprendersi in modo coordinato e rafforzare la cooperazione con la NATO per garantire la complementarità delle misure. Dovrebbe essere letta congiuntamente alle relazioni mensili sui progressi compiuti verso la creazione di un'autentica ed efficace Unione della sicurezza.

2. RICONOSCERE LA NATURA IBRIDA DI UNA MINACCIA

Le attività ibride sono sempre più frequenti nel contesto europeo della sicurezza. L'intensità di tali attività cresce di pari passo con l'aumento di timori di interferenze nelle elezioni, campagne di disinformazione, attività informatiche dolose e tentativi, da parte degli autori di atti ibridi, di radicalizzare i membri più vulnerabili della società per farne i propri mandatari. Le vulnerabilità alle minacce ibride non sono limitate ai confini nazionali, pertanto è necessaria una risposta coordinata anche a livello di UE e NATO. Gli sviluppi a partire dall'aprile 2016 evidenziano che, sebbene le minacce siano ancora spesso valutate isolatamente, nell'Unione si riconoscono e comprendono sempre più la natura ibrida di alcune

[5] Tabella di marcia di Bratislava del Consiglio europeo, del 16 settembre 2016, e dichiarazione di Roma dei leader dei 27 Stati membri e del Consiglio europeo, del Parlamento europeo e della Commissione europea, del 25 marzo 2017.
[6] http://www.consilium.europa.eu/it/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation/.
[7] Documento di riflessione della Commissione sul futuro della difesa europea, del 7.6.2017: https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_it.pdf.

delle attività osservate e la necessità di un'azione coordinata. L'UE continuerà a profondere sforzi per migliorare la consapevolezza situazionale e la cooperazione.

***Azione 1* — Gli Stati membri, sostenuti se del caso dalla Commissione e dall'Alto rappresentante, sono invitati a procedere a uno studio sui rischi ibridi per individuare le vulnerabilità principali, nonché specifici indicatori delle minacce ibride, che possono interessare strutture e reti nazionali e paneuropee.**

Il Consiglio ha istituito un Gruppo degli amici della presidenza, che riunisce esperti degli Stati membri al fine di creare uno strumento di indagine generale che li aiuti a individuare i principali indicatori delle minacce ibride, a integrarli nei meccanismi di allarme rapido e di valutazione dei rischi esistenti nonché a condividerli ove opportuno. Il mandato è già stato stabilito e i lavori sono già iniziati. Lo strumento di indagine generale dovrebbe essere pronto entro la fine del 2017, in vista dell'inizio delle indagini poco dopo. La protezione contro le minacce ibride dovrebbe essere realizzata in modo sinergico: poiché le indagini forniranno informazioni preziose sulla portata della vulnerabilità e della preparazione in Europa, gli Stati membri sono invitati a realizzarle al più presto.

a. MIGLIORARE LA CONOSCENZA

La condivisione delle attività di analisi e valutazione dell'intelligence costituisce uno strumento essenziale per ridurre l'incertezza e rafforzare la consapevolezza situazionale. Nell'ultimo anno sono stati compiuti progressi significativi. È stata costituita la cellula dell'UE per l'analisi delle minacce ibride, ora pienamente operativa, è stata istituita la task force East StratCom e la Finlandia ha creato il centro europeo per la lotta contro le minacce ibride. I lavori si sono in gran parte concentrati sull'analisi degli strumenti e delle leve della disinformazione o della propaganda e si sono avvalsi della buona cooperazione esistente tra la task force East StratCom dell'UE, la cellula per l'analisi delle minacce ibride e la NATO. Si tratta di una buona base per portare avanti la costruzione di una cultura più radicata dell'analisi e della valutazione della natura ibrida delle minacce alla nostra sicurezza interna ed esterna.

Cellula per l'analisi delle minacce ibride

***Azione 2* — Creazione di una cellula dell'UE per l'analisi delle minacce ibride presso l'esistente struttura del centro dell'UE di analisi dell'intelligence, in grado di ricevere ed esaminare informazioni riservate e pubbliche sulle minacce ibride. Gli Stati membri sono invitati a istituire punti di contatto nazionali sulle minacce ibride per garantire la cooperazione e una comunicazione sicura con tale cellula.**

La cellula dell'UE per l'analisi delle minacce ibride è stata costituita in seno al centro dell'UE di analisi dell'intelligence al fine di ricevere ed esaminare informazioni riservate e pubbliche provenienti da varie parti interessate sulle minacce ibride. Le analisi sono successivamente condivise nell'UE e tra gli Stati membri e alimentano il processo decisionale dell'UE, anche contribuendo alla valutazione dei rischi relativi alla sicurezza a livello dell'UE. La direzione "intelligence" dello Stato maggiore dell'Unione europea contribuisce con l'analisi militare all'attività della cellula per l'analisi delle minacce ibride. A oggi sono stati prodotti oltre 50 valutazioni e briefing relativi alle minacce ibride. Dal gennaio 2017 la cellula realizza un bollettino di informazione periodico sulle minacce ibride che analizza le minacce e le

problematiche attuali ed è direttamente condiviso con le istituzioni e gli organi dell'UE e i punti di contatto nazionali[8]. La piena capacità operativa della cellula è stata raggiunta, come previsto, nel maggio 2017. Sono inoltre in corso attività di condivisione a livello del personale con la nuova sezione della NATO per l'analisi delle minacce ibride, che interessano sia gli insegnamenti appresi nella creazione della cellula per l'analisi delle minacce ibride sia le informazioni (nel pieno rispetto delle norme dell'UE sullo scambio di informazioni riservate). La cellula dell'UE per l'analisi delle minacce ibride sta attualmente vagliando ulteriori iniziative intese a potenziare la cooperazione futura e rivestirà un ruolo fondamentale negli esercizi paralleli UE-NATO in programma per l'autunno 2017, con i quali si metterà alla prova la capacità di risposta della cellula dell'UE per l'analisi delle minacce ibride per applicare in seguito gli insegnamenti appresi.

Comunicazione strategica

Azione 3 — L'Alto rappresentante e gli Stati membri studieranno insieme delle modalità di aggiornamento e coordinamento delle capacità per la formulazione di comunicazioni strategiche proattive e per ottimizzare il ricorso a specialisti del controllo dei media e a esperti linguisti.

Tra le misure utilizzate per danneggiare gli avversari, negli ultimi mesi è aumentato il ricorso alle campagne di disinformazione e alla diffusione sistematica di notizie false sui social media. Laddove i social media sono la piattaforma più utilizzata, informazioni apparentemente affidabili e legittime possono influenzare l'opinione pubblica a vantaggio di alcuni individui, organizzazioni o governi. Queste tattiche ibride perseguono l'obiettivo più ampio di generare confusione nelle nostre società e screditare i governi democratici e le loro strutture, istituzioni ed elezioni. Le notizie false sono spesso diffuse tramite piattaforme online (cfr. anche l'azione 17). La Commissione e l'Alto rappresentante accolgono con favore le recenti iniziative adottate dalle piattaforme e dalle fonti di informazione online per combattere la disinformazione. La Commissione continuerà a promuovere l'adozione di analoghe misure volontarie.

L'Alto rappresentante ha istituito la task force East StratCom, che formula previsioni e reagisce alle campagne e ai casi di disinformazione, migliorando sensibilmente la comunicazione sulle politiche dell'Unione e rafforzando l'ambiente mediatico nei paesi del vicinato orientale. Negli ultimi due anni la task force ha portato alla luce più di 3 000 casi di disinformazione in 18 lingue. L'imminente lancio del nuovo sito web "*#EUvsdisinformation*", dotato di uno strumento di ricerca online, migliorerà considerevolmente l'accesso degli utenti. Le attività di ricerca e analisi mostrano tuttavia che il numero dei canali di disinformazione e dei messaggi diffusi quotidianamente è notevolmente superiore. Il progetto EU-STRAT, finanziato da Orizzonte 2020, analizza la politica e i media nei paesi del partenariato orientale.

L'Alto rappresentante invita gli Stati membri a sostenere l'operato delle task force StratCom per contrastare più efficacemente l'aumento delle minacce ibride. In questo modo si aiuterà la task force di comunicazione strategica per il Sud a migliorare le attività di comunicazione e sensibilizzazione nel mondo arabo, anche in lingua araba, a sfatare miti e a fare chiarezza sui fatti riguardanti l'Unione europea e le sue politiche. L'interazione con i giornalisti locali contribuirà ad assicurare che i contenuti siano in sintonia con la cultura locale. Entrambe le

[8] A oggi 21 Stati membri hanno designato punti di contatto nazionali. Si tratta di persone con responsabilità nel campo delle politiche o della resilienza nelle capitali degli Stati membri.

task force, sostenute dalla cellula dell'UE per l'analisi delle minacce ibride, mirano ad assecondare e integrare le attività degli Stati membri in materia. Inoltre la Commissione cofinanzia la Rete europea per la comunicazione strategica, una rete collaborativa di 26 Stati membri che condivide analisi, buone pratiche e idee sull'uso delle comunicazioni strategiche nella lotta contro l'estremismo violento e sulla disinformazione.

Centro di eccellenza per la "lotta contro le minacce ibride"

***Azione 4* — Gli Stati membri sono invitati a prendere in considerazione l'opportunità di istituire un centro di eccellenza per la "lotta contro le minacce ibride".**

Rispondendo all'invito a istituire un centro di eccellenza, nell'aprile 2017 la Finlandia ha creato il centro europeo per la lotta contro le minacce ibride. Dieci Stati membri dell'UE[9], la Norvegia e gli Stati Uniti ne sono membri, mentre l'Unione europea e la NATO sono state invitate a sostenere il comitato direttivo[10]. La missione del centro prevede la promozione del dialogo strategico e la realizzazione di attività di ricerca e analisi a fianco delle comunità di interesse per migliorare la resilienza e la capacità di risposta al fine di contribuire a contrastare le minacce ibride. Dovrebbe inoltre fungere da sede per gli esercizi futuri in materia. Le attività del centro dovrebbero essere complementari a quelle della cellula dell'UE per l'analisi delle minacce ibride, con cui è già in stretto contatto. L'UE sta vagliando le modalità per assicurare al centro sostegno concreto.

b. RAFFORZARE LA RESILIENZA

Il Quadro congiunto pone la resilienza (ad esempio per quanto concerne i trasporti, le comunicazioni, l'energia, i sistemi finanziari e le infrastrutture di sicurezza regionali) al centro dell'azione dell'UE volta a resistere alla propaganda e alle campagne di disinformazione, ai tentativi di danneggiare le imprese, le società e i flussi economici nonché agli attacchi alle tecnologie dell'informazione e ai sistemi informatici. Esso considera il rafforzamento della resilienza un'azione preventiva e dissuasiva per consolidare le società ed evitare l'aggravarsi di crisi all'interno e all'esterno dell'UE. Il valore aggiunto dell'intervento nell'UE consiste nell'assistere gli Stati membri e i partner nel rafforzamento della loro resilienza facendo leva su una vasta gamma di programmi e strumenti esistenti. Sono stati compiuti progressi importanti per quanto riguarda le azioni per rafforzare la resilienza in settori come la cibersicurezza, le infrastrutture critiche, la protezione contro gli usi illeciti dei sistemi finanziari e la lotta contro l'estremismo violento e la radicalizzazione.

Proteggere le infrastrutture critiche

***Azione 5* — La Commissione, in cooperazione con gli Stati membri e le parti interessate, individuerà strumenti comuni, compresi indicatori, per migliorare la protezione e la resilienza delle infrastrutture critiche a fronte delle minacce ibride nei settori rilevanti.**

Nel contesto del programma europeo per la protezione delle infrastrutture critiche (EPCIP), la Commissione ha portato avanti i lavori intesi a individuare strumenti comuni, compresi indicatori di vulnerabilità, per migliorare la resilienza delle infrastrutture critiche a fronte delle minacce ibride nei settori rilevanti. Nel maggio 2017 la Commissione ha organizzato un

[9] Finlandia, Francia, Germania, Lettonia, Lituania, Polonia, Svezia, Regno Unito, Estonia e Spagna.
[10] Il centro è aperto alla partecipazione degli altri Stati membri dell'UE e degli alleati della NATO.

seminario sulle minacce ibride alle infrastrutture critiche che ha visto la partecipazione di quasi tutti gli Stati membri, degli operatori delle infrastrutture critiche, della cellula dell'UE per l'analisi delle minacce ibride e della NATO in qualità di osservatore. Nel corso del seminario sono state concordate una tabella di marcia comune e azioni da intraprendere per il futuro sulla base di un questionario inviato alle autorità nazionali degli Stati membri. La Commissione consulterà nuovamente le parti interessate in autunno, con l'obiettivo di trovare un accordo sugli indicatori entro la fine del 2017.

L'Agenzia europea per la difesa sta lavorando per individuare le lacune in termini di ricerca e capacità comuni derivanti dalla connessione tra le infrastrutture energetiche e le capacità di difesa. Nell'autunno 2017 redigerà un documento concettuale e preparerà una serie di azioni pilota per lo sviluppo di metodologie olistiche.

Aumentare la sicurezza dell'approvvigionamento energetico dell'UE

Azione 6 — La Commissione, in cooperazione con gli Stati membri, sosterrà gli sforzi per diversificare le fonti di energia e per promuovere norme di sicurezza e protezione volte ad aumentare la resilienza delle infrastrutture nucleari.

Nel dicembre 2016 la Commissione ha formulato proposte concrete nel pacchetto sulla sicurezza dell'approvvigionamento e nell'aprile 2017 il Consiglio e il Parlamento europeo hanno raggiunto un accordo sul nuovo regolamento sulla sicurezza dell'approvvigionamento di gas, inteso a scongiurare l'insorgenza di crisi nell'approvvigionamento di gas. Le nuove norme assicureranno un approccio comune e coordinato a livello regionale alle misure di sicurezza dell'approvvigionamento tra gli Stati membri. Grazie a esse, l'Europa potrà essere più preparata e gestire più efficacemente le carenze di gas in caso di crisi o di attacco ibrido. Per la prima volta si applicherà il principio di solidarietà: gli Stati membri potranno aiutare i vicini in caso di attacco o crisi grave in modo che le famiglie e le imprese europee non siano colpite da black-out.

L'UE ha inoltre compiuto progressi nello sviluppo di progetti chiave per diversificare rotte e fonti energetiche in linea con la strategia quadro per l'Unione dell'energia e la strategia europea di sicurezza energetica. Ad esempio, sono in corso lavori di costruzione nel corridoio meridionale di trasporto del gas per tutti i principali progetti di gasdotti: espansione del gasdotto del Caucaso meridionale e dei gasdotti transanatolico e transadriatico, espansione a monte dello Shah Deniz II ed espansione del corridoio meridionale di trasporto del gas all'Asia centrale, in particolare al Turkmenistan. Le importazioni di gas naturale liquefatto (GNL) in Europa sono in aumento e provengono da nuove fonti, quali gli USA. L'esempio del terminale in Lituania evidenzia come i progetti di diversificazione possono ridurre la dipendenza da un unico fornitore. Anche intensificare gli sforzi nel campo dell'energia e utilizzare meglio le fonti energetiche autoctone, in particolare le fonti rinnovabili, contribuisce alla diversificazione delle rotte e delle fonti energetiche.

Nell'area della sicurezza nucleare, la Commissione sostiene attivamente, in particolare organizzando seminari con le autorità nazionali e i regolatori, l'attuazione coerente ed efficace delle due direttive sulla sicurezza nucleare e sulle norme fondamentali di sicurezza, che gli Stati membri sono tenuti a recepire entro la fine, rispettivamente, del 2017 e del 2018. Anche il programma Euratom di ricerca e formazione contribuisce a incrementare la sicurezza nucleare.

Sicurezza dei trasporti e della catena di approvvigionamento

***Azione 7* — La Commissione monitorerà le minacce emergenti nel settore dei trasporti e aggiornerà se del caso la legislazione. Nell'attuare la strategia UE per la sicurezza marittima e la strategia UE di gestione dei rischi doganali con i relativi piani d'azione, la Commissione e l'Alto rappresentante (nell'ambito delle loro rispettive competenze), in coordinamento con gli Stati membri, esamineranno come rispondere alle minacce ibride, in particolare quelle relative alle infrastrutture critiche nel settore dei trasporti.**

In linea con la comunicazione relativa all'Unione della sicurezza, la Commissione agevola la valutazione dei rischi relativi alla sicurezza a livello dell'UE con gli Stati membri, il centro dell'UE di analisi dell'intelligence e le agenzie competenti per individuare le minacce alla sicurezza dei trasporti e sostenere lo sviluppo di misure di attenuazione efficaci e proporzionate. L'abbattimento del volo Malaysia Airlines MH17 nei cieli dell'Ucraina orientale nel 2014 ha posto in evidenza i rischi connessi al sorvolo delle zone di conflitto. In linea con le raccomandazioni della task force europea ad alto livello sulle zone di conflitto[11], la Commissione ha elaborato, con il sostegno di esperti nazionali dei settori dell'aviazione e della sicurezza e del SEAE, una metodologia di "valutazione del rischio comune dell'UE" che consente lo scambio di informazioni riservate e la definizione di un quadro del rischio comune. Nel marzo 2017 l'Agenzia europea per la sicurezza aerea (AESA) ha pubblicato il primo "bollettino di informazione sulle zone di conflitto"[12] sulla base dei risultati di tale valutazione del rischio comune dell'UE. La Commissione sta vagliando l'espansione delle attività di valutazione del rischio condotte nell'ambito della sicurezza aerea ad altre modalità di trasporto (ad esempio ferroviario e marittimo) e formulerà proposte in materia nel 2018. Nel giugno 2017 la Commissione, il SEAE e gli Stati membri hanno avviato un esercizio di valutazione del rischio sulla sicurezza ferroviaria al fine di individuare lacune ed elaborare possibili misure di attenuazione dei rischi.

Anche nell'ambito dei progetti di ricerca nel settore della sicurezza del Settimo programma quadro e di Orizzonte 2020 sono stati compiuti sforzi considerevoli in materia di sicurezza aerea e gestione del traffico aereo (ATM). Nel campo dell'aviazione civile la Commissione, congiuntamente all'Agenzia europea per la sicurezza aerea e alle parti interessate, sta sviluppando due iniziative intese a rafforzare la cibersicurezza, anche affrontando le minacce ibride: l'istituzione della squadra di pronto intervento informatico in materia di aviazione e la creazione di una task force per la cibersicurezza nell'ambito dell'impresa comune per la ricerca sulla gestione del traffico aereo nel cielo unico europeo (SESAR), responsabile per la gestione del traffico aereo nel cielo unico europeo. L'Agenzia europea per la difesa offre contributi militari per quanto concerne la cibersicurezza aerea all'impresa comune SESAR e all'Agenzia europea per la sicurezza aerea tramite la piattaforma europea di coordinamento strategico sulla cibersicurezza che, su richiesta degli Stati membri e dell'industria, sosterrà il coordinamento a livello dell'UE di tutte le attività nel settore dell'aviazione. In linea con la tabella di marcia per la cibersicurezza nell'aviazione, nel 2016 l'Agenzia europea per la sicurezza aerea ha condotto analisi delle lacune delle norme vigenti, in particolare per quanto concerne la definizione e l'istituzione dello *European Centre for Cybersecurity in Aviation* (centro europeo per la cibersicurezza nell'aviazione). Quest'ultimo è ormai operativo e collabora con la squadra di pronto intervento informatico dell'UE (CERT-EU) (il protocollo di

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf.
[12] https://ad.easa.europa.eu/czib-docs/page-1.

intesa è stato firmato nel febbraio 2017), realizzando analisi delle minacce nell'aviazione, e con EUROCONTROL (è stata adottata una tabella di marcia per la cooperazione); è stato inoltre sviluppato un sito web per la distribuzione di analisi delle fonti aperte. Entro l'autunno 2017 saranno adottati un programma di standardizzazione e un sistema per lo scambio sicuro di informazioni.

Gestione dei rischi doganali

Per quanto concerne le dogane, la Commissione intende potenziare significativamente il sistema di informazioni anticipate sui carichi e di gestione dei rischi doganali. Il sistema contempla l'intera gamma dei rischi doganali, anche in relazione alle minacce alla sicurezza e all'integrità delle catene di approvvigionamento internazionali e alle infrastrutture critiche rilevanti (ad esempio minacce dirette, poste dalle importazioni, agli impianti portuali marittimi, agli aeroporti o alle frontiere terrestri). Il potenziamento mira a garantire che le dogane dell'UE ottengano tutte le informazioni necessarie dagli operatori per quanto riguarda la circolazione delle merci, che siano in grado di condividere tali informazioni in maniera più efficace tra gli Stati membri, che applichino le norme comuni e le norme specifiche degli Stati membri in materia di rischio e che siano in grado di identificare più efficacemente le spedizioni ad alto rischio cooperando in maniera più intensiva con altre autorità, in particolare altre agenzie per la sicurezza e l'applicazione della legge. Lo sviluppo IT richiesto per l'attuazione del potenziamento da parte della Commissione è attualmente nella fase iniziale e nei prossimi mesi saranno avviati i pertinenti investimenti a livello centrale.

Spazio

Azione 8 — Nel contesto della strategia spaziale e del piano di azione europeo in materia di difesa, la Commissione proporrà di incrementare la resilienza delle infrastrutture spaziali contro le minacce ibride, in particolare attraverso un eventuale ampliamento dell'ambito della sorveglianza dello spazio e del tracciamento per coprire le minacce ibride, la preparazione della prossima generazione di GovSatCom a livello europeo e l'introduzione di Galileo nelle infrastrutture critiche che dipendono dalla sincronizzazione oraria.

La Commissione, nel predisporre il quadro normativo relativo alla comunicazione satellitare governativa (GovSatCom) e alla sorveglianza dello spazio e al tracciamento nel 2018, integrerà aspetti della resilienza contro le minacce ibride nella sua valutazione. In linea con la strategia spaziale, nel preparare l'evoluzione di Galileo e Copernicus la Commissione valuterà le potenzialità di tali servizi in termini di contributo all'attenuazione della vulnerabilità delle infrastrutture critiche. La relazione di valutazione dovrebbe essere pronta nell'autunno 2017 e la proposta sulla prossima generazione di Copernicus e Galileo è prevista per il 2018. L'Agenzia europea per la difesa lavora a progetti collaborativi di sviluppo delle capacità nelle aree delle comunicazioni spaziali, della navigazione, della sincronizzazione e del posizionamento per scopi militari e dell'osservazione della Terra. Tutti i progetti si concentreranno su requisiti di resilienza alla luce delle minacce ibride attuali ed emergenti.

Capacità di difesa

Azione 9 — L'Alto rappresentante, sostenuto se del caso dagli Stati membri, in collaborazione con la Commissione, proporrà progetti relativi alle possibilità di adattamento delle capacità di difesa e al loro sviluppo in modo pertinente per l'UE, per lottare specificamente contro le minacce ibride verso uno o più Stati membri.

Nel 2016 e nel 2017 l'Agenzia europea per la difesa ha condotto tre esercizi di simulazione concernenti scenari di minacce ibride congiuntamente alla Commissione, al SEAE e ad esperti degli Stati membri. Le conclusioni confluiranno nella revisione del piano di sviluppo delle capacità in modo che gli sviluppi in termini di capacità chiave richiesti per contrastare le minacce ibride siano integrati nelle nuove priorità di sviluppo delle capacità dell'UE. Il lavoro di revisione del catalogo dei requisiti 2005 terrà conto della dimensione ibrida delle minacce. Nell'aprile 2017 l'Agenzia europea per la difesa ha completato una relazione di analisi sulle implicazioni militari degli attacchi ibridi alle infrastrutture critiche dei porti, che sarà discussa nel corso di un seminario con esperti marittimi nell'ottobre 2017. Un'altra analisi specifica del ruolo del settore militare nel contesto della lotta contro i mini-droni è prevista per il 2018. Inoltre le priorità in termini di capacità individuate dagli Stati membri ai fini del rafforzamento della resilienza contro le minacce ibride potrebbero essere ammissibili al sostegno nell'ambito del Fondo europeo per la difesa dal 2019. La Commissione invita i colegislatori ad assicurare una rapida adozione e gli Stati membri a presentare proposte di progetti in materia di capacità per rafforzare la resilienza dell'UE contro le minacce ibride.

***Azione 10* — La Commissione, in cooperazione con gli Stati membri, aumenterà la conoscenza delle minacce ibride e la resilienza a queste nell'ambito degli esistenti meccanismi di preparazione e coordinamento, in particolare del comitato per la sicurezza sanitaria.**

Al fine di rafforzare la preparazione e la resilienza nei confronti delle minacce ibride, compreso lo sviluppo di capacità nei sistemi sanitari e alimentari, la Commissione sostiene gli Stati membri tramite formazione ed esercizi di simulazione, favorendo lo scambio di linee guida basate sull'esperienza e finanziando azioni comuni. Tali attività sono portate avanti in particolare nel quadro di sicurezza sanitaria dell'UE relativo alle gravi minacce per la salute a carattere transfrontaliero e nell'ambito del programma di salute pubblica per l'attuazione del regolamento sanitario internazionale, un pilastro legislativo vincolante per 196 paesi, compresi gli Stati membri, che mira a prevenire e contrastare a livello globale i gravi rischi per la salute pubblica a carattere transfrontaliero. Per valutare la preparazione e la capacità di risposta trasversali nel settore sanitario, i servizi della Commissione realizzeranno un esercizio sulle minacce ibride complesse e multidimensionali nell'autunno 2017. La Commissione e gli Stati membri stanno preparando un'azione comune in materia di vaccinazione, comprendente la previsione dell'offerta e della domanda di vaccini e la ricerca sui processi innovativi di fabbricazione al fine di rafforzare l'offerta di vaccini e migliorare la sicurezza sanitaria a livello dell'UE (2018-2020). La Commissione collabora inoltre con l'Autorità europea per la sicurezza alimentare e il Centro europeo per la prevenzione e il controllo delle malattie ai fini dell'adeguamento alle tecniche avanzate di ricerca scientifica, per consentire di identificare più precisamente le minacce per la salute e la loro origine e, di conseguenza, gestire rapidamente le emergenze inerenti alla sicurezza alimentare. La Commissione ha istituito una rete di finanziatori della ricerca (*Global Research Collaboration for Infectious Disease Preparedness*) per garantire una risposta coordinata della ricerca entro 48 ore dall'insorgenza di un focolaio significativo.

***Azione 11* — La Commissione incoraggia gli Stati membri, come questione prioritaria, a costituire e utilizzare appieno una rete fra i 28 CSIRT e la CERT-UE (squadra di pronto intervento informatico dell'UE), così come un quadro per la cooperazione strategica. La Commissione, in coordinamento con gli Stati membri, dovrebbe garantire che le iniziative di settore sulle minacce informatiche (ad es. aviazione, settore energetico, settore marittimo) siano coerenti con le capacità intersettoriali coperte dalla direttiva NIS per mettere insieme informazioni, competenze e reazioni rapide.**

I recenti attacchi informatici a livello mondiale, che mediante ransomware e malware hanno disattivato migliaia di sistemi informatici, hanno nuovamente evidenziato l'urgente necessità di rafforzare la resilienza informatica e le azioni di sicurezza all'interno dell'UE. Come annunciato nella revisione intermedia della strategia per il mercato unico digitale, la Commissione e l'Alto rappresentante stanno attualmente rivedendo la strategia dell'UE per la cibersicurezza del 2013, in particolare con l'adozione di un pacchetto previsto per settembre 2017. L'obiettivo sarà quello di fornire una risposta più efficace e intersettoriale a queste minacce, al fine di aumentare la fiducia nella società e nell'economia digitali. Sarà inoltre riesaminato il mandato dell'ENISA, l'Agenzia dell'UE per la sicurezza delle reti e dell'informazione, al fine di definire il suo ruolo nel mutato ecosistema della cibersicurezza. Il Consiglio europeo[13] ha accolto con favore l'intenzione della Commissione di rivedere la strategia per la cibersicurezza.

L'adozione della direttiva sulla sicurezza delle reti e i sistemi informativi[14] (NIS) nel luglio 2016 ha rappresentato una misura fondamentale volta a consolidare la resilienza della cibersicurezza su scala europea. La direttiva stabilisce le prime norme a livello di UE in materia di cibersicurezza, migliora le capacità in questo settore e rafforza la cooperazione tra gli Stati membri. Essa prescrive inoltre alle imprese che operano in settori critici di adottare adeguate misure di sicurezza e di segnalare gli incidenti informatici gravi alla competente autorità nazionale. Tra i settori critici rientrano energia, trasporti, acqua, sanità, banche e infrastruttura dei mercati finanziari. I mercati online, i servizi di cloud computing e i motori di ricerca dovranno adottare misure analoghe. Un'attuazione coerente in diversi settori nonché a livello transfrontaliero sarà garantita dal gruppo di cooperazione sulla sicurezza delle reti e dei servizi informativi (istituito dalla Commissione nel 2016), che ha il compito di evitare la frammentazione del mercato. In tale contesto, la direttiva sulla sicurezza delle reti e dei sistemi informativi è considerata il quadro di riferimento per tutte le iniziative settoriali in materia di cibersicurezza. La direttiva istituisce inoltre la rete di gruppi di intervento per la sicurezza informatica in caso di incidente ("CSIRT"), che riunisce tutte le pertinenti parti interessate. Parallelamente la Commissione e la CERT-UE procedono a un attivo monitoraggio delle minacce informatiche e allo scambio di informazioni con le autorità nazionali al fine di garantire che i sistemi informatici delle istituzioni dell'UE siano sicuri e resilienti agli attacchi informatici. Nel maggio 2017 l'incidente causato dal ransomware WannaCry ha rappresentato la prima occasione per la rete di impegnarsi nello scambio operativo di informazioni e nella cooperazione grazie alla diffusione di raccomandazioni. La squadra di pronto intervento informatico dell'UE ha inoltre mantenuto uno stretto contatto con il Centro europeo per la lotta alla criminalità informatica ("EC3") di Europol, i gruppi di intervento per la sicurezza informatica in caso di incidente dei paesi colpiti ("CSIRT"), le unità specializzate nella lotta alla criminalità informatica e i principali partner del settore per attenuare la minaccia e assistere le vittime. Il fatto di scambiare relazioni nazionali sulla situazione ha prodotto una consapevolezza situazionale comune in tutta l'UE. Questa esperienza ha permesso alla rete di essere meglio preparata ai successivi incidenti (ad esempio, "NonPetya"). Sono stati inoltre individuati diversi problemi attualmente in fase di soluzione.

[13] Conclusioni del Consiglio europeo del 22-23 giugno 2017.

[14] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

Azione 12 *— La Commissione, in coordinamento con gli Stati membri, lavorerà con l'industria nel contesto di un partenariato pubblico-privato contrattuale sulla cibersicurezza, per sviluppare e testare tecnologie volte a proteggere maggiormente gli utenti e le infrastrutture dagli aspetti informatici delle minacce ibride.*

Nel luglio 2016 la Commissione, in coordinamento con gli Stati membri, ha firmato con l'industria un partenariato pubblico-privato contrattuale sulla cibersicurezza (PPP contrattuale), che nel quadro del programma di ricerca e innovazione Orizzonte 2020 investe fino a 450 milioni di euro per sviluppare e testare tecnologie volte a proteggere maggiormente gli utenti e le infrastrutture da minacce informatiche e ibride. Il partenariato ha prodotto il primo programma strategico di ricerca paneuropeo, volto a consolidare la resilienza delle infrastrutture critiche e dei cittadini agli attacchi informatici. Il partenariato ha aumentato il coordinamento tra le parti interessate, migliorando l'efficienza e l'efficacia dei finanziamenti per la cibersicurezza nell'ambito di Orizzonte 2020. Parallelamente il partenariato si occupa di questioni connesse alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione così come delle modalità per sopperire alla forte carenza nel mercato di professionisti qualificati in cibersicurezza. Considerato il sostanziale fabbisogno di ricerca civile e l'elevato livello di resilienza necessario nella difesa, il gruppo di ricerca e tecnologie informatiche dell'Agenzia europea per la difesa apporta il suo contributo nei settori di ricerca individuati dall'Organizzazione europea per la cibersicurezza nella sua agenda strategica di ricerca e innovazione.

Azione 13 *— La Commissione pubblicherà orientamenti destinati ai detentori di risorse della rete intelligente per migliorare la cibersicurezza dei loro impianti. Nel contesto dell'iniziativa sull'assetto del mercato dell'energia, la Commissione valuterà l'opportunità di proporre "piani di preparazione ai rischi" e regole procedurali per scambiarsi le informazioni e garantire la solidarietà fra gli Stati membri nei periodi di crisi, comprese norme su come prevenire e mitigare gli attacchi informatici*.

Nel settore dell'energia la Commissione sta preparando una strategia settoriale sulla cibersicurezza con l'istituzione della piattaforma per la cibersicurezza degli esperti di energia per rafforzare l'attuazione della direttiva NIS. Uno studio del febbraio 2017 ha individuato le migliori tecniche disponibili per rafforzare il livello della cibersicurezza dei sistemi di misurazione intelligenti, offrendo così sostegno alla piattaforma. La Commissione ha inoltre istituito una piattaforma web "Centro dell'UE per lo scambio di informazioni sugli incidenti e le minacce", che analizza e condivide informazioni sulle minacce e sugli incidenti informatici nel settore dell'energia.

Accrescere la resilienza del settore finanziario nei confronti delle minacce ibride

Azione 14 *— La Commissione, in cooperazione con l'ENISA[15], con gli Stati membri, con le autorità competenti internazionali, europee e nazionali e con le istituzioni finanziarie, promuoverà e faciliterà le piattaforme e le reti di scambio di informazioni sulle minacce e affronterà i fattori che ostacolano la condivisione di tali informazioni.*

Riconoscendo che le minacce informatiche costituiscono uno dei rischi principali per la stabilità finanziaria, la Commissione ha esaminato il quadro normativo sui servizi di pagamento nell'Unione europea, che attualmente è in fase di attuazione. La direttiva riveduta

[15] Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione.

sui servizi di pagamento[16] ha introdotto nuove disposizioni per migliorare la sicurezza degli strumenti di pagamento e l'autenticazione forte del cliente al fine di ridurre le frodi, in particolare nei pagamenti online. Il nuovo quadro legislativo sarà applicabile dal gennaio 2018. Attualmente la Commissione, assistita dall'Autorità bancaria europea, e in consultazione con le parti interessate, sta elaborando norme tecniche di regolamentazione, che dovrebbero essere pubblicate entro la fine del 2017, in materia di autenticazione forte del cliente nonché di comunicazione comune e sicura per garantire la sicurezza delle operazioni di pagamento. Sul fronte internazionale la Commissione ha inoltre lavorato in stretta cooperazione con i rispettivi partner del G7 alla definizione dei "principi fondamentali del G7 sulla cibersicurezza nel settore finanziario" approvati nell'ottobre 2016 dai ministri delle finanze e dai governatori delle banche centrali. I principi sono destinati ai soggetti del settore finanziario (privati e pubblici) e favoriscono un approccio coordinato alla cibersicurezza nel settore finanziario per far fronte congiuntamente alle minacce informatiche, comprese quelle più gravi e sofisticate.

Trasporti

Azione 15 — La Commissione e l'Alto rappresentante (nell'ambito delle rispettive competenze), in coordinamento con gli Stati membri, esamineranno come rispondere in particolare alle minacce ibride relative agli attacchi informatici nel settore dei trasporti.

L'attuazione del piano d'azione relativo alla strategia per la sicurezza marittima dell'UE[17] contribuirà ad eliminare la mentalità a compartimenti stagni nello scambio di informazioni e promuoverà un uso di risorse condiviso tra autorità civili e militari. Un approccio amministrativo globale ha portato a una maggiore cooperazione in vari settori. Entro la fine del 2017 dovrebbe essere completato un programma congiunto, civile e militare, della Commissione e del SEAE in materia di ricerca strategica nel settore della sicurezza, con un workshop finale sulla protezione delle infrastrutture marittime critiche. Questi lavori potrebbero in futuro essere ampliati in modo da coprire le minacce emergenti, connesse a interferenze oltre il confine delle acque nazionali e riguardanti le condotte sottomarine, il trasferimento di energia e il cablaggio per la comunicazione tradizionale e in fibra ottica.

Un recente studio[18] ha esaminato la capacità di valutazione dei rischi delle autorità nazionali che svolgono funzioni di guardia costiera. Lo studio ha individuato i principali ostacoli alla collaborazione e ha raccomandato modalità pratiche per migliorare la cooperazione tra autorità marittime a livello di UE e nazionale in questo ambito specifico. La valutazione dei rischi è essenziale nella lotta contro le minacce marittime ed è ancor più determinante ai fini della stima e della prevenzione delle minacce ibride, poiché queste ultime richiedono considerazioni supplementari e più complesse. I risultati dello studio saranno presentati a diversi forum dei servizi di guardia costiera affinché le raccomandazioni proposte possano essere valutate e attuate per accrescere la cooperazione in questo settore, tenendo conto dell'obiettivo principale di preparazione e risposta alla minacce ibride.

---

[16] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno (GU L 337 del 23.12.2015, pag. 35).

[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf e la seconda relazione sull'attuazione del piano d'azione EUMSS (Strategia per la sicurezza marittima dell'UE) presentata agli Stati membri il 21 giugno 2017.

[18] Studio *Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions*, 2017 https://ec.europa.eu/maritimeaffairs/documentation/studies.

Contrastare il finanziamento al terrorismo

Azione 16 — La Commissione sfrutterà l'attuazione del piano d'azione contro il finanziamento del terrorismo anche per contribuire alla lotta contro le minacce ibride.

Gli autori di minacce ibride e i loro sostenitori hanno bisogno di fondi per realizzare i propri piani. L'impegno dell'UE contro il finanziamento della criminalità e del terrorismo nel quadro dell'agenda europea sulla sicurezza e del piano d'azione contro il finanziamento del terrorismo può contribuire anche alla lotta contro le minacce ibride. Nel dicembre 2016, la Commissione ha presentato tre proposte legislative, che riguardavano tra l'altro sanzioni penali in materia di riciclaggio di denaro e di pagamenti illeciti in contanti nonché il congelamento e la confisca dei beni[19].
Tutti gli Stati membri erano tenuti a recepire entro il 26 giugno 2017 la 4ª direttiva antiriciclaggio[20] e nel luglio 2016 la Commissione ha presentato una proposta legislativa mirata al fine di integrare e rafforzare detta direttiva con ulteriori misure[21].

Il 26 giugno la Commissione ha presentato la valutazione sovranazionale dei rischi prevista per la 4ª direttiva antiriciclaggio. Ha inoltre presentato una proposta di regolamento volto a prevenire l'importazione e lo stoccaggio nell'UE di beni culturali illegalmente esportati da paesi terzi[22]. Entro l'anno la Commissione presenterà una relazione sulla sua valutazione in corso circa la necessità di eventuali misure supplementari per tracciare il finanziamento del terrorismo nell'UE; essa è altresì impegnata in una revisione della normativa in materia di lotta contro le frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti[23].

L'Ottava relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza fornisce ulteriori dettagli sullo stato di attuazione del piano d'azione contro il finanziamento del terrorismo.

Promuovere i valori comuni dell'UE e società inclusive, aperte e resilienti

Rafforzare la resilienza contro la radicalizzazione e l'estremismo violento

La radicalizzazione religiosa e ideologica e i conflitti etnici e tra minoranze possono essere istigati da attori esterni tramite il sostegno a gruppi specifici o mediante sforzi per alimentare i conflitti tra gruppi. Sono emerse nuove sfide, quali le minacce da parte di attori solitari, i nuovi percorsi di radicalizzazione, potenzialmente anche nel contesto della crisi migratoria, nonché l'aumento dell'estremismo di destra (compresa la violenza contro i migranti) e il rischio di polarizzazioni. Sebbene i lavori sulla radicalizzazione siano portati avanti nel

[19] Terza relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza, COM(2016) 831 final.
[20] Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione (GU L 141 del 5.6.2015, pag. 73).
[21] Per maggiori dettagli si veda la Terza relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2016) 831 final) e l'Ottava relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza (COM(2017) 354 final).
[22] COM(2017) 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final 0.
[23] Ottava relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza, COM(2017) 354 final.

contesto dell'Unione della sicurezza, tali lavori possono essere rilevanti anche indirettamente per le minacce ibride poiché le persone vulnerabili alla radicalizzazione possono essere manipolate dagli autori di minacce ibride.

Azione 17* — *La Commissione sta attuando le azioni contro la radicalizzazione presentate nell'agenda europea sulla sicurezza e sta analizzando la necessità di rafforzare le procedure di eliminazione dei contenuti illegali da Internet, invitando gli intermediari alla dovuta diligenza nella gestione delle reti e dei sistemi.

Prevenzione della radicalizzazione

La Commissione continua ad attuare la sua strategia di risposta multiforme alla radicalizzazione di cui alla comunicazione "Sostenere la prevenzione della radicalizzazione che porta all'estremismo violento"[24] del giugno 2016, che stabilisce azioni chiave, quali la promozione di un'istruzione inclusiva e di valori comuni, il contrasto della propaganda estremistica online e della radicalizzazione nelle carceri, l'intensificazione della cooperazione con paesi terzi e il potenziamento della ricerca per comprendere meglio il carattere evolutivo della radicalizzazione e favorire risposte strategiche più informate. La rete di sensibilizzazione al problema della radicalizzazione (RAN) è stata il fulcro dei lavori della Commissione volti a sostenere gli Stati membri in questo settore, in collaborazione con gli operatori locali a livello di comunità. Ulteriori dettagli sono forniti nell'Ottava relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza[25].

Radicalizzazione online e incitazione all'odio

Conformemente all'agenda europea sulla sicurezza[26], la Commissione ha preso provvedimenti per ridurre la disponibilità di contenuti illegali online, in particolare mediante l'unità UE addetta alle segnalazioni su Internet di Europol e il Forum dell'UE su Internet[27]. Sono stati compiuti progressi significativi anche nel quadro del codice di condotta volto a contrastare l'illecito incitamento all'odio online[28]. Ulteriori dettagli sono forniti nell'Ottava relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza[29]. Tali azioni saranno rafforzate anche alla luce delle conclusioni del Consiglio europeo[30], del vertice del G7[31] e del vertice del G20[32].

Le piattaforme online svolgono un ruolo determinante nell'affrontare i contenuti illegali o potenzialmente dannosi. Nell'ambito della strategia per il mercato unico digitale, illustrata

[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf
[25] COM(2017) 354 final
[26] Per maggiori dettagli si veda l'Ottava relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza, COM(2017) 354 final.
[27] Per maggiori dettagli si veda l'Ottava relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza, COM(2017) 354 final.
[28] Codice di condotta sull'illecito incitamento all'odio, 31 maggio 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[29] Per maggiori dettagli si veda l'Ottava relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza, COM(2017) 354 final.
[30] Conclusioni del Consiglio del 22-23 giugno 2016.
[31] Vertice del G7 di Taormina, Italia, 26-27/05/2017.
[32] Vertice del G20 di Amburgo, Germania, 07-08/07/2017.

nella revisione intermedia[33], la Commissione garantirà un migliore coordinamento dei dialoghi con le piattaforme incentrati sui meccanismi e sulle soluzioni tecniche in materia di rimozione dei contenuti illegali. Ove pertinente, l'obiettivo dovrebbe essere quello di sostenere tali meccanismi con orientamenti su aspetti quali la notifica e la rimozione di contenuti illegali. La Commissione fornirà inoltre orientamenti sulle norme in materia di responsabilità.

Maggiore cooperazione con i paesi terzi

Azione 18 — L'Alto rappresentante, in coordinamento con la Commissione, organizzerà uno studio sui rischi ibridi nelle regioni del vicinato. L'Alto rappresentante, la Commissione e gli Stati membri si avvarranno degli strumenti a loro disposizione per rafforzare le capacità dei partner e aumentare la loro resilienza alle minacce ibride. Potrebbero essere realizzate missioni PSDC, autonome o come complemento agli strumenti dell'UE, per aiutare i partner a consolidare le loro capacità.

L'Unione europea si è concentrata maggiormente sul rafforzamento delle capacità e della resilienza nei paesi partner nel settore della sicurezza, basandosi fra l'altro sulla connessione fra sicurezza e sviluppo, potenziando la dimensione della sicurezza della politica europea di vicinato riveduta e avviando dialoghi sulla sicurezza e sul contrasto al terrorismo con i paesi del Mediterraneo. A tale riguardo è stato avviato, come progetto pilota, uno studio sui rischi in cooperazione con la Repubblica di Moldova. Lo studio ha l'obiettivo di contribuire a individuare le principali vulnerabilità del paese e ad assicurare che l'assistenza dell'UE sia destinata specificamente a tali settori. I risultati del progetto pilota hanno dimostrato che lo studio stesso è stato considerato utile. Basandosi sull'esperienza acquisita, la Commissione e il SEAE raccomanderanno di dare la priorità alle azioni nell'ambito della promozione dell'efficacia, della comunicazione strategica, della protezione delle infrastrutture critiche e della cibersicurezza.

Prossimamente altri paesi vicini potrebbero beneficiare dello studio sulla base di questa prima esperienza, seppur con adattamenti mirati per tenere conto delle diverse situazioni nazionali locali e di minacce specifiche e per evitare sovrapposizioni con i dialoghi in corso in materia di sicurezza e di contrasto al terrorismo. Più in generale, il 7 luglio 2017 la Commissione e l'Alto rappresentante hanno adottato una comunicazione congiunta su "Un approccio strategico alla resilienza nell'azione esterna dell'UE"[34]. L'obiettivo è quello di sostenere i paesi partner a diventare più resilienti alle attuali sfide globali. La comunicazione riconosce la necessità di abbandonare gli obiettivi di contenimento delle crisi per orientarsi verso un approccio alle vulnerabilità più strutturale e di lungo termine, focalizzato sulla previsione, sulla prevenzione e sulla preparazione.

Resilienza informatica per lo sviluppo

L'UE sostiene i paesi all'esterno dell'Europa, al fine di rafforzare la resilienza delle loro reti di informazione. La crescente digitalizzazione presenta un'intrinseca dimensione di sicurezza che comporta particolari problemi per la resilienza delle reti di informazione a livello mondiale, poiché gli attacchi informatici non conoscono frontiere. L'UE sostiene i paesi terzi

[33]Cfr. la comunicazione della Commissione COM(2017) 228 final.
[34]Comunicazione congiunta al Parlamento europeo e al Consiglio: Un approccio strategico alla resilienza nell'azione esterna dell'UE, JOIN (2017) 21 final.

nello sviluppo della loro capacità di prevenire e di rispondere adeguatamente in caso di guasti accidentali e di attacchi informatici. Facendo seguito a un progetto pilota sulla cibersicurezza del 2016 nell'ex Repubblica jugoslava di Macedonia, nel Kossovo[35] e nella Moldova, la Commissione avvierà un nuovo programma volto a migliorare la resilienza informatica dei paesi terzi, principalmente in Africa e in Asia, ma anche in Ucraina, nel periodo 2017-2020. Il programma mira ad accrescere la sicurezza e la preparazione delle reti e delle infrastrutture critiche di informazione nei paesi terzi sulla base di un approccio amministrativo globale, garantendo nel contempo il rispetto dei diritti umani e dello Stato di diritto.

Sicurezza aerea

L'aviazione civile resta un bersaglio importante ed emblematico per i terroristi, ma potrebbe anche essere presa di mira nell'ambito di campagne ibride. Mentre l'UE ha sviluppato un solido quadro di sicurezza del trasporto aereo, i voli provenienti da paesi terzi possono dimostrarsi più vulnerabili. Conformemente alla risoluzione 2309 (2016) del Consiglio di sicurezza delle Nazioni Unite, la Commissione sta intensificando gli sforzi per rafforzare le capacità dei paesi terzi. Nel gennaio 2017 la Commissione ha avviato una nuova valutazione integrata dei rischi per assicurare la definizione delle priorità e il coordinamento degli sforzi volti allo sviluppo delle capacità compiuti a livello dell'UE e degli Stati membri, così come con partner internazionali. Nel 2016 la Commissione ha avviato un progetto quadriennale sulla sicurezza dell'aviazione civile in Africa e nella penisola arabica per contrastare la minaccia del terrorismo per l'aviazione civile. Il progetto è incentrato sulla condivisione di competenze tra Stati partner ed esperti degli Stati membri della Conferenza europea dell'aviazione civile, nonché su attività di tutoraggio, formazione e accompagnamento. Le attività saranno ulteriormente potenziate nel corso del 2017.

c. PREVENZIONE, RISPOSTA ALLE CRISI E RIPRESA

Se le conseguenze possono essere mitigate da politiche a lungo termine a livello nazionale e dell'UE, nel breve termine resta fondamentale rafforzare la capacità degli Stati membri e dell'Unione di prevenire le minacce ibride, reagirvi e riprendersi in modo rapido e coordinato. Una risposta rapida agli eventi provocati dalle minacce ibride è fondamentale. Nel corso dell'ultimo anno si sono compiuti notevoli progressi in questo settore, in particolare ora è in vigore nell'UE un protocollo operativo che definisce il processo di gestione delle crisi in caso di attacchi ibridi. In futuro si svolgeranno regolarmente attività di monitoraggio ed esercizi.

Azione 19 — L'Alto rappresentante e la Commissione, in coordinamento con gli Stati membri, definiranno un protocollo operativo comune e procederanno a esercizi regolari per migliorare la capacità decisionale strategica in risposta alle minacce ibride complesse, basandosi sulle procedure di gestione delle crisi e sui dispositivi integrati dell'UE per la risposta politica alle crisi.

Il Quadro congiunto ha raccomandato l'istituzione di meccanismi di risposta rapida agli eventi provocati dalle minacce ibride al fine di coordinare nell'UE i meccanismi di risposta[36] e i

[35] Tale designazione non pregiudica le posizioni riguardo allo status ed è in linea con la risoluzione 1244 (1999) del Consiglio di sicurezza delle Nazioni Unite e con il parere della Corte internazionale di giustizia sulla dichiarazione di indipendenza del Kosovo.

[36] I dispositivi integrati dell'UE per la risposta politica alle crisi (IPCR) del Consiglio, il sistema ARGUS della Commissione e il CRM del SEAE.

sistemi di allarme rapido. A tal fine i servizi della Commissione e il SEAE hanno pubblicato il protocollo operativo dell'UE per contrastare le minacce ibride (Manuale tattico dell'UE)[37], che delinea le modalità di coordinamento, fusione e analisi dell'intelligence, informazione per i processi di definizione delle politiche, esercitazione e formazione così come di cooperazione con le organizzazioni partner, in particolare la NATO, in caso di minacce ibride. Analogamente la NATO ha elaborato un manuale tattico su una maggiore interazione NATO-UE per la prevenzione e il contrasto delle minacce ibride in materia di ciberdifesa, comunicazione strategica, consapevolezza situazionale e gestione delle crisi. Il manuale tattico dell'UE sarà testato in un esercizio nell'autunno 2017 nel quadro degli esercizi paralleli e coordinati che prevedono l'interazione con la NATO.

Azione 20 — La Commissione e l'Alto rappresentante, nell'ambito dei rispettivi settori di competenza, esamineranno l'applicabilità e le implicazioni pratiche dell'articolo 222 del TFUE e dell'articolo 42, paragrafo 7, del TUE in caso di attacchi ibridi gravi e di vasta portata.

L'articolo 42, paragrafo 7, del TUE prevede disposizioni in caso di aggressione armata nel territorio di uno Stato membro, mentre l'articolo 222 del TFUE prevede disposizioni (clausola di solidarietà) applicabili se uno Stato membro è oggetto di un attacco terroristico o è colpito da una calamità naturale o provocata dall'uomo. In caso di attacchi ibridi, che sono una combinazione di azioni criminali e sovversive, è più probabile il ricorso all'articolo 222. L'invocazione della clausola di solidarietà comporta il coordinamento a livello del Consiglio [dispositivi integrati per la risposta politica alle crisi (IPCR)] e l'intervento delle istituzioni, delle agenzie e degli organismi pertinenti dell'UE, nonché i programmi e i meccanismi di assistenza dell'UE. La decisione 2014/415/UE del Consiglio prevede modalità di attuazione da parte dell'Unione della clausola di solidarietà. Tali modalità di applicazione restano valide e non occorre rivedere la decisione del Consiglio. Se un attacco ibrido comprende un'aggressione armata, potrebbe inoltre essere invocato l'articolo 42, paragrafo 7. In quest'ultimo caso l'aiuto e l'assistenza sono forniti sia dagli Stati membri sia dall'UE. La Commissione e l'Alto rappresentante continueranno a valutare le modalità più efficaci per far fronte a tali attacchi.

L'adozione del protocollo operativo dell'UE di cui sopra sostiene direttamente tale valutazione e il protocollo sarà applicato nel quadro degli esercizi paralleli e coordinati dell'UE (PACE) nell'ottobre 2017. Gli esercizi testeranno i vari meccanismi dell'UE e la sua capacità di interagire al fine di accelerare il processo decisionale quando l'ambiguità dovuta a una minaccia ibrida riduce la chiarezza.

Azione 21 — L'Alto rappresentante, in coordinamento con gli Stati membri, integrerà, utilizzerà e coordinerà le capacità di azione militare nella lotta contro le minacce ibride nell'ambito della politica di sicurezza e di difesa comune.

In risposta al compito di integrare le capacità militari per sostenere la PESC/PSDC e in seguito a un seminario con esperti militari del dicembre 2016 e agli orientamenti del gruppo del comitato militare dell'Unione europea nel maggio 2017, è stato completato nel luglio 2017 il parere sul contributo militare dell'UE alla lotta contro le minacce ibride nell'ambito della PSDC che sarà portato avanti mediante il piano di sviluppo e attuazione di concetti.

[37] Documento di lavoro dei servizi della Commissione (2016) 227, adottato il 7 luglio 2016.

d. COOPERAZIONE UE-NATO

<u>Azione 22</u> — L'Alto rappresentante, in coordinamento con la Commissione, porterà avanti il dialogo informale e rafforzerà la cooperazione e il coordinamento con la NATO sulla consapevolezza situazionale, la comunicazione strategica, la cibersicurezza e la "prevenzione e risposta alle crisi" ai fini della lotta contro le minacce ibride, nel rispetto dei principi di inclusione e di autonomia decisionale di ciascuna organizzazione.

Sulla base della dichiarazione congiunta firmata l'8 luglio 2016 a Varsavia dai presidenti del Consiglio europeo e della Commissione europea e dal segretario generale dalla NATO, l'UE e la NATO hanno sviluppato un insieme comune di 42 proposte di attuazione, successivamente approvate in sviluppi distinti e paralleli il 6 dicembre 2016 da entrambi i Consigli dell'UE e della NATO[38]. Nel luglio 2017 l'Alto rappresentante/Vicepresidente e il Segretario generale della NATO hanno pubblicato una relazione sui progressi complessivi compiuti nell'attuazione delle 42 azioni della dichiarazione congiunta. La lotta alle minacce ibride è uno dei sette settori di cooperazione individuati nella dichiarazione congiunta e riguarda dieci delle 42 azioni. La relazione dimostra che gli sforzi congiunti intrapresi nell'ultimo anno hanno prodotto risultati sostanziali. Molte delle azioni specifiche intese a contrastare le minacce ibride sono già state menzionate, tra cui il centro europeo di eccellenza per la lotta contro le minacce ibride, una migliore consapevolezza situazionale, l'istituzione della cellula dell'UE per l'analisi delle minacce ibride e la sua interazione con la nuova sezione della NATO per l'analisi delle minacce ibride, così come la collaborazione tra i gruppi per la comunicazione strategica. Per la prima volta, il personale della NATO e quello dell'UE effettueranno esercitazioni congiunte su come rispondere a uno scenario ibrido. Si prevede che l'esercitazione testerà l'attuazione di oltre un terzo delle proposte comuni. L'Unione europea effettuerà i propri esercizi paralleli e coordinati quest'anno e si prepara ad assumere un ruolo guida nel 2018.

In materia di resilienza, il personale dell'UE e quello della NATO si sono impegnati in briefing incrociati, anche sul dispositivo dell'UE di risposta politica integrata alle crisi. I contatti regolari tra il personale dell'UE e quello della NATO, anche attraverso seminari o tramite la partecipazione al comitato direttivo dell'Agenzia europea per la difesa, hanno consentito scambi di informazioni sui requisiti di base della NATO relativi alla resilienza a livello nazionale. Ulteriori scambi fra la Commissione e la NATO per rafforzare la resilienza sono previsti nell'autunno. La prossima relazione sulla cooperazione UE-NATO proporrà possibilità di ampliare la cooperazione tra le due organizzazioni.

3. CONCLUSIONE

Il Quadro congiunto presenta azioni volte a contribuire alla lotta contro le minacce ibride e a rafforzare la resilienza a livello dell'UE, nazionale e dei partner. La Commissione e l'Alto rappresentante hanno raggiunto risultati in tutti gli ambiti, in stretta cooperazione con gli Stati membri e i partner, tuttavia è importante non perdere lo slancio a fronte delle minacce ibride attuali, in costante evoluzione. Spetta agli Stati membri la responsabilità principale della lotta contro le minacce ibride attinenti alla sicurezza nazionale e al mantenimento dell'ordine pubblico. La resilienza nazionale e gli sforzi collettivi volti a proteggere dalle minacce ibride devono essere intesi come elementi di un unico sforzo complessivo che si rafforzano a

[38] http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/

vicenda. Gli Stati membri sono pertanto invitati a realizzare al più presto studi sui rischi ibridi che forniranno informazioni preziose sulla portata della vulnerabilità e della preparazione in Europa. Sulla base dei progressi significativi registrati nel migliorare la consapevolezza occorrerebbe ottimizzare il potenziale della cellula dell'UE per l'analisi delle minacce ibride. L'Alto rappresentante invita gli Stati membri a sostenere l'operato delle task force StratCom per contrastare più efficacemente l'aumento delle minacce ibride. L'UE sosterrà pienamente il centro europeo per la lotta contro le minacce ibride con sede in Finlandia.

Il punto di forza dell'intervento nell'UE consiste nell'assistere gli Stati membri e i partner nel rafforzamento della loro resilienza sulla base di una vasta gamma di programmi e strumenti esistenti. Sono stati compiuti progressi importanti per quanto riguarda le azioni intese a rafforzare la resilienza in settori come i trasporti, l'energia, la cibersicurezza, le infrastrutture critiche, la protezione contro gli usi illeciti dei sistemi finanziari e la lotta contro l'estremismo violento e la radicalizzazione. L'azione dell'UE volta a rafforzare la resilienza continuerà, poiché la natura delle minacce ibride è in evoluzione. In particolare, l'UE svilupperà indicatori per migliorare la protezione e la resilienza delle infrastrutture critiche a fronte delle minacce ibride nei settori pertinenti.

Il Fondo europeo per la difesa può cofinanziare, assieme agli Stati membri, le priorità in termini di capacità per rafforzare la resilienza alle minacce ibride. L'imminente pacchetto sulla cibersicurezza, così come le misure intersettoriali volte all'attuazione della direttiva sulla sicurezza delle reti e dei servizi informativi, costituiranno nuove piattaforme per contrastare le minacce ibride all'interno dell'UE.

La Commissione e l'Alto rappresentante invitano gli Stati membri e le parti interessate, ogni qual volta sia necessario, a raggiungere rapidamente un accordo e garantire una rapida ed efficace attuazione delle diverse misure volte a rafforzare la resilienza delineate nella presente comunicazione. L'UE consoliderà e approfondirà la già proficua cooperazione con la NATO.

L'Unione conferma il proprio impegno a mobilitare tutti i pertinenti strumenti dell'UE per affrontare le minacce ibride complesse. Sostenere gli sforzi degli Stati membri resta una priorità per l'Unione, che agisce in qualità di garante della sicurezza più forte e reattivo, assieme ai suoi partner principali.