COMMISSIONE
EUROPEA

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

Bruxelles, 6.4.2016
JOIN(2016) 18 final

# COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO

## Quadro congiunto per contrastare le minacce ibride

## La risposta dell'Unione europea

## 1. INTRODUZIONE

Negli ultimi anni, la situazione della sicurezza nell'Unione europea è cambiata radicalmente. Le grandi sfide alla pace e alla stabilità nel vicinato orientale e meridionale dell'UE continuano a mettere in evidenza la necessità, per l'Unione, di adattare e aumentare le sue capacità come garante della sicurezza, mettendo fortemente l'accento sulla stretta relazione fra la sicurezza esterna e interna. Molte delle attuali sfide alla pace, alla sicurezza e alla prosperità derivano dall'instabilità dell'immediato vicinato dell'UE e dalle diverse forme che assumono le minacce. Negli Orientamenti politici del 2014, il Presidente della Commissione europea Jean-Claude Juncker ha sottolineato la necessità di "lavorare su un'Europa più forte quando si tratta di questioni di sicurezza e di difesa" e di combinare gli strumenti europei e nazionali in modo più efficace che in passato. Oltre a ciò, a seguito dell'invito formulato dal Consiglio Affari esteri del 18 maggio 2015, l'Alto rappresentante, in stretta cooperazione con i servizi della Commissione e con l'Agenzia europea per la Difesa (AED) e consultando gli Stati membri dell'UE, ha intrapreso i lavori per presentare questo Quadro congiunto corredato di proposte praticabili per contribuire a contrastare le minacce ibride e rafforzare la resilienza dell'UE e dei suoi Stati membri nonché dei partner[1]. Nel giugno 2015 il Consiglio europeo ha ribadito la necessità di mobilitare gli strumenti dell'UE per contribuire a contrastare le minacce ibride[2].

Se le definizioni delle "minacce ibride" variano e devono rimanere flessibili per rispondere al loro carattere mutevole, il concetto intende invece esprimere la combinazione di attività coercitive e sovversive, di metodi convenzionali e non convenzionali (cioè diplomatici, militari, economici e tecnologici), che possono essere usati in modo coordinato da entità statali o non statali per raggiungere determinati obiettivi, rimanendo però sempre al di sotto della soglia di una guerra ufficialmente dichiarata. L'accento è generalmente messo sullo sfruttamento dei punti deboli del bersaglio, e sulla creazione di ambiguità per ostacolare il processo decisionale. Le campagne massicce di disinformazione, che usano i media sociali per controllare il discorso politico o per radicalizzare, reclutare e dirigere mandatari, possono essere vettori di minacce ibride.

Nella misura in cui la lotta contro le minacce ibride attiene alla sicurezza e alla difesa nazionale e al mantenimento dell'ordine pubblico, la responsabilità principale ricade sugli Stati membri, poiché la maggior parte delle vulnerabilità nazionali sono specifiche dei singoli paesi. Tuttavia, molti Stati membri dell'UE devono far fronte a minacce comuni, che possono interessare anche reti o infrastrutture transfrontaliere. Tali minacce possono essere affrontate più efficacemente con una risposta coordinata a livello europeo, avvalendosi delle politiche e degli strumenti dell'UE e contando sulla solidarietà europea, sull'assistenza reciproca e su tutto il potenziale del trattato di Lisbona. Le politiche e gli strumenti dell'UE possono svolgere — e di fatto già svolgono in ampia misura — un

[1] Conclusioni del Consiglio sulla politica di sicurezza e di difesa comune (PSDC), maggio 2015 [Consilium 8971/15]
[2] Conclusioni del Consiglio europeo, giugno 2015 [EUCO 22/15].

grande ruolo di valore aggiunto nel lavoro di sensibilizzazione, che sta contribuendo ad accrescere la resilienza degli Stati membri nella risposta alle minacce comuni. L'azione esterna dell'UE proposta nell'ambito del presente Quadro è guidata dai principi di cui all'articolo 21 del trattato sull'Unione europea (TUE), fra cui figurano la democrazia, lo Stato di diritto, l'universalità e l'indivisibilità dei diritti dell'uomo e il rispetto dei principi della Carta delle Nazioni Unite e del diritto internazionale[3].

La presente comunicazione congiunta intende facilitare un approccio olistico che permetterà all'UE, in coordinamento con gli Stati membri, di lottare in modo specifico contro le minacce di natura ibrida, creando sinergie fra tutti gli strumenti pertinenti e promuovendo una stretta cooperazione fra tutti gli interlocutori competenti[4]. Le azioni si basano su strategie e politiche settoriali esistenti che contribuiscono all'instaurazione di una maggiore sicurezza. In particolare, l'agenda europea sulla sicurezza[5], la strategia globale dell'Unione europea in materia di politica estera e di sicurezza e il piano di azione europeo in materia di difesa (in via d'elaborazione)[6], la strategia dell'Unione europea per la cibersicurezza,[7] la strategia europea di sicurezza energetica[8] e la strategia per la sicurezza marittima dell'Unione europea[9] sono strumenti che possono a loro volta contribuire alla lotta contro le minacce ibride.

Poiché anche la NATO sta lavorando alla lotta contro le minacce ibride e il Consiglio Affari esteri ha proposto di intensificare la cooperazione e il coordinamento in questo settore, alcune delle proposte sono volte a rafforzare la cooperazione UE-NATO nella lotta contro le minacce ibride.

La risposta proposta si articola intorno ai seguenti elementi: maggiore conoscenza della situazione, rafforzamento della resilienza, prevenzione e risposta alle crisi e ripresa.

## 2. RICONOSCERE LA NATURA IBRIDA DI UNA MINACCIA

Le minacce ibride mirano a sfruttare i punti deboli di un paese e spesso cercano di minare i valori democratici e le libertà fondamentali. Come primo passo, l'Alto rappresentante e la Commissione lavoreranno insieme agli Stati membri per migliorare la conoscenza della situazione con un controllo e una valutazione dei rischi che possono colpire le vulnerabilità dell'UE. La Commissione sta mettendo a punto metodi di valutazione dei rischi per la sicurezza per contribuire ad alimentare il processo decisionale e per

[3] La Carta dei diritti fondamentali dell'UE è vincolante per le istituzioni e per gli Stati membri quando danno attuazione al diritto dell'Unione.
[4] Eventuali proposte legislative dovranno rispondere ai requisiti stabiliti dalla Commissione ai fini di una migliore regolamentazione, in linea con gli orientamenti della Commissione per legiferare meglio, SWD(2015)111.
[5] COM(2015)185 final.
[6] Da presentarsi nel 2016.
[7] Si vedano il quadro strategico dell'UE in materia di ciberdifesa [Consilium 15585/14] e la comunicazione congiunta "Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro", febbraio 2013 [JOIN(2013)1].
[8] Comunicazione congiunta sulla strategia europea di sicurezza energetica, maggio 2014 [SWD(2014) 330].
[9] Comunicazione congiunta "Per un settore marittimo globale aperto e sicuro: elementi di una strategia per la sicurezza marittima dell'Unione europea" — JOIN(2014)9 final — 6.3.2014.

promuovere l'elaborazione di politiche basate sui rischi in settori che vanno dalla sicurezza aerea al finanziamento del terrorismo e al riciclaggio di denaro. Sarebbe inoltre utile che gli Stati membri procedessero a uno studio volto a recensire i settori vulnerabili alle minacce ibride. Lo scopo sarebbe quello di individuare gli indicatori delle minacce ibride, di integrarli nei meccanismi di allarme rapido e di valutazione dei rischi esistenti, e di condividerli se del caso.

***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.**

## 3. ORGANIZZARE LA RISPOSTA DELL'UE — MIGLIORARE LA CONOSCENZA DELLA SITUAZIONE

### 3.1. Cellula dell'UE per l'analisi delle minacce ibride

È fondamentale che l'UE, coordinandosi con gli Stati membri, abbia un livello sufficiente di conoscenza della situazione che consenta di individuare eventuali cambiamenti nel settore della sicurezza legati ad attività ibride da parte di entità statali e/o non statali. Per contrastare efficacemente le minacce ibride, è importante migliorare lo scambio di informazioni e promuovere una pertinente condivisione dei dati di intelligence fra tutti i settori e fra l'Unione europea, i suoi Stati membri e i partner.

Una cellula dell'UE per l'analisi delle minacce ibride rappresenterà un punto focale unico per l'esame di tali minacce, istituito presso il centro dell'UE di analisi dell'intelligence (EU INTCEN) del Servizio europeo per l'azione esterna (SEAE). Tale cellula dovrebbe ricevere, analizzare e condividere informazioni riservate e pubbliche specificamente legate a indicatori e allarmi di minacce ibride provenienti da varie parti interessate del SEAE (comprese le delegazioni dell'UE), la Commissione (con le agenzie dell'UE[10]) e gli Stati membri. In collegamento con organismi analoghi esistenti a livello dell'UE[11] e a livello nazionale, la cellula dovrebbe studiare gli aspetti esterni delle minacce ibride che interessano l'UE e il suo vicinato, per analizzare rapidamente gli incidenti rilevanti e alimentare il processo decisionale strategico dell'UE, anche contribuendo alla valutazione dei rischi relativi alla sicurezza svolta a livello dell'UE. I risultati analitici della cellula dovranno essere trattati e utilizzati conformemente alle norme UE sulla protezione dei dati e delle informazioni riservate[12]. La cellula dovrebbe collaborare con gli organismi esistenti a livello UE e nazionale, e gli Stati membri dovrebbero istituire punti di contatto nazionali ad essa collegati. Il personale all'interno e all'esterno dell'UE (compreso quello assegnato a delegazioni, operazioni o missioni dell'UE) e negli Stati membri dovrebbe essere inoltre formato a riconoscere i segnali precoci di minacce ibride.

[10] Conformemente ai loro mandati.
[11] Ad esempio il centro europeo per la lotta alla criminalità informatica e il centro antiterrorismo di Europol, Frontex e la squadra di pronto intervento informatico dell'UE (CERT-EU).
[12] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995.

***<u>Azione 2</u> — Creazione di una cellula dell'UE per l'analisi delle minacce ibride presso l'esistente struttura EU INTCEN, 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.***

### 3.2. Comunicazione strategica

Gli autori delle minacce ibride possono fare sistematicamente opera di disinformazione, anche con campagne mirate sui media sociali, cercando di radicalizzare le persone, destabilizzare la società e controllare il discorso politico. È fondamentale saper rispondere alle minacce ibride predisponendo una solida tattica di **comunicazione strategica**. Fornire rapide risposte fattuali e fare opera di sensibilizzazione sulle minacce ibride sono importanti fattori di rafforzamento della resilienza sociale.

La comunicazione strategica dovrebbe sfruttare appieno gli strumenti dei media sociali così come i tradizionali mezzi audiovisivi e on-line. Il SEAE, basandosi sulle attività delle task force East Stratcom e Arab Stratcom, dovrebbe ottimizzare il ricorso a linguisti esperti di lingue importanti non-UE e a specialisti di media sociali, in grado di seguire le informazioni al di fuori dell'UE e di garantire una comunicazione mirata per reagire alla disinformazione. Gli Stati membri dovrebbero inoltre elaborare meccanismi coordinati di comunicazione strategica per sostenere l'indicazione delle fonti e contrastare la disinformazione onde mettere a nudo le minacce ibride.

***<u>Azione 3</u> — 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.***

### 3.3. Centro di eccellenza per la "lotta contro le minacce ibride"

Basandosi sull'esperienza di alcuni Stati membri e organizzazioni partner[13], un ente multinazionale o una rete di enti multinazionali potrebbero fungere da centro di eccellenza per la lotta contro le minacce ibride. Un tale centro potrebbe concentrarsi sullo studio delle modalità di attuazione delle minacce ibride, e potrebbe favorire l'elaborazione di nuovi concetti e tecnologie nel settore privato e nell'industria per aiutare gli Stati membri nel rafforzamento della resilienza. Questo lavoro di ricerca potrebbe contribuire ad allineare le politiche, le dottrine e i concetti europei e nazionali, e a garantire che i processi decisionali tengano conto delle complessità e ambiguità legate alle minacce ibride. Il centro dovrebbe elaborare programmi per far progredire la ricerca ed esercizi per trovare soluzioni pratiche ai problemi esistenti posti dalle minacce ibride. La forza di un centro di questo tipo si baserebbe sulle competenze sviluppate dalle persone che vi partecipano, di varie nazionalità e settori, civili e militari, privati ed accademici.

[13] Centri di eccellenza della NATO.

Il centro potrebbe operare in stretta collaborazione con i centri di eccellenza esistenti dell'UE[14] e della NATO[15] per attingere alle conoscenze sulle minacce ibride acquisite grazie alla difesa informatica, alla comunicazione strategica, alla cooperazione civile-militare, alla risposta energetica e alla reazione alle crisi.

***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".**

## 4. ORGANIZZARE LA RISPOSTA DELL'UE — RAFFORZARE LA RESILIENZA

La resilienza è la capacità di resistere allo stress e di riprendersi, rafforzati dal fatto di aver fatto fronte alle sfide. Per lottare efficacemente contro le minacce ibride, occorre concentrarsi sulle potenziali vulnerabilità delle infrastrutture chiave, delle catene di approvvigionamento e della società. Basandosi sugli strumenti e sulle politiche dell'Unione è possibile rendere più resilienti le infrastrutture a livello UE.

### 4.1. Proteggere le infrastrutture critiche

Proteggere le infrastrutture critiche (ad es. le catene di approvvigionamento energetico e i trasporti) è importante, poiché un attacco non convenzionale perpetrato da autori di minacce ibride su qualsiasi "obiettivo non strategico" potrebbe portare a gravi disfunzionamenti a livello economico o sociale. Per garantire la protezione in tale ambito, il programma europeo per la protezione delle infrastrutture critiche[16] (EPCIP) prevede un approccio sistemico intersettoriale multirischio, imperniato sulle interdipendenze e basato sulla realizzazione di attività nell'ambito degli assi di intervento in materia di prevenzione, preparazione e risposta. La direttiva sulle infrastrutture critiche europee[17] stabilisce una procedura per l'individuazione e la designazione delle infrastrutture critiche europee (ECI) e un approccio comune per la valutazione della necessità di migliorarne la protezione. In particolare, occorrerebbe rilanciare i lavori avviati nel quadro di tale direttiva per rafforzare la resilienza delle infrastrutture critiche relative ai trasporti (ad es. i principali aeroporti e porti mercantili dell'UE). La Commissione valuterà l'opportunità di elaborare strumenti comuni, compresi indicatori, per aumentare la resilienza delle infrastrutture critiche a fronte delle minacce ibride in tutti i settori rilevanti.

***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.**

---

[14] Ad esempio l'Istituto dell'UE per gli studi sulla sicurezza (EU ISS) e i centri d'eccellenza tematici dell'UE sulle questioni CBRN.

[15] http://www.nato.int/cps/en/natohq/topics_68372.htm

[16] Comunicazione della Commissione relativa a un programma europeo per la protezione delle infrastrutture critiche, 12.12.2006, COM(2006)786 final.

[17] Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, GU L 345 del 23.12.2008.

### *4.1.1. Reti energetiche*

È di importanza vitale per l'UE che la produzione e la distribuzione di energia non vengano perturbate: grosse interruzioni dell'alimentazione potrebbero essere dannose. Un aspetto essenziale della lotta contro le minacce ibride è continuare a diversificare le fonti d'energia dell'UE, i fornitori e le rotte, per garantire approvvigionamenti energetici più sicuri e resilienti. La Commissione sta inoltre procedendo a delle valutazioni dei rischi e della sicurezza ("prove di stress") presso le centrali elettriche dell'UE. Per assicurare la diversificazione energetica, i lavori nel quadro della strategia dell'Unione dell'energia sono in via di intensificazione: a titolo d'esempio si può citare il corridoio meridionale del gas, che può permettere di trasportare gas dalla regione del Caspio in Europa, e, nell'Europa del nord, la predisposizione di hub di gas liquidi con molteplici fornitori. Questo esempio dovrebbe essere seguito nell'Europa centrale e orientale e nel Mediterraneo, dove un hub del gas è in corso di sviluppo[18]. Lo sviluppo del mercato del gas naturale liquefatto contribuirà anch'esso positivamente alla realizzazione di questo obiettivo.

Per quanto riguarda i materiali e gli impianti nucleari, la Commissione sostiene l'elaborazione e l'adozione delle più rigorose norme di sicurezza, rafforzando così la resilienza. La Commissione sta premendo per il recepimento e l'attuazione coerenti della direttiva per la sicurezza nucleare[19], che stabilisce norme per la prevenzione degli incidenti e l'attenuazione delle loro conseguenze, e delle disposizioni della direttiva sulle norme fondamentali di sicurezza[20] relative alla cooperazione internazionale in materia di preparazione alle emergenze e intervento in caso di emergenza, in particolare fra Stati membri vicini e con i paesi vicini.

***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.***

### *4.1.2 Sicurezza dei trasporti e della catena di approvvigionamento*

I trasporti sono fondamentali per il funzionamento dell'Unione. Gli attacchi ibridi alle infrastrutture dei trasporti (come gli aeroporti, le infrastrutture stradali, i porti e le ferrovie) possono avere gravi conseguenze e perturbare gli spostamenti e le catene di approvvigionamento. Nell'attuazione della legislazione relativa alla sicurezza del trasporto aereo e marittimo[21] la Commissione procede a ispezioni periodiche[22] e, con i

[18] Sui progressi finora realizzati si veda lo stato dell'Unione dell'energia 2015 (COM(2015)572 final).
[19] Direttiva 2009/71/Euratom del Consiglio, del 25 giugno 2009, che istituisce un quadro comunitario per la sicurezza nucleare degli impianti nucleari, modificata dalla direttiva 2014/87/Euratom del Consiglio dell'8 luglio 2014.
[20] Direttiva 2013/59/Euratom del Consiglio, del 5 dicembre 2013, che stabilisce norme fondamentali di sicurezza relative alla protezione contro i pericoli derivanti dall'esposizione alle radiazioni ionizzanti, e che abroga le direttive 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom e 2003/122/Euratom.
[21] Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002; regolamento di esecuzione (UE) 2015/1998 della Commissione, del 5 novembre 2015, che stabilisce disposizioni particolareggiate per l'attuazione delle norme fondamentali comuni sulla sicurezza

suoi lavori sulla sicurezza del trasporto terrestre, intende far fronte alle minacce ibride emergenti. In tale contesto, un quadro dell'UE è in corso di discussione nell'ambito del regolamento rivisto sulla sicurezza aerea[23], che rientra nella strategia per l'aviazione in Europa[24]. Inoltre, le minacce alla sicurezza marittima vengono affrontate nell'ambito della strategia per la sicurezza marittima dell'Unione europea e del relativo piano d'azione[25]. Quest'ultimo consente all'UE e agli Stati membri di affrontare in maniera esaustiva le sfide poste alla sicurezza marittima, compresa la lotta alle minacce ibride, attraverso una cooperazione intersettoriale fra interlocutori civili e militari per proteggere le infrastrutture critiche marittime, la catena d'approvvigionamento globale, il commercio marittimo e le risorse energetiche e naturali marittime. La sicurezza della catena d'approvvigionamento internazionale viene inoltre affrontata nella strategia UE di gestione dei rischi doganali e nel relativo piano d'azione[26].

***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 col relativo piano 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**.

### *4.1.3 Spazio*

Le minacce ibride potrebbero avere ad oggetto le infrastrutture spaziali, con conseguenze multisettoriali. L'UE ha istituito un quadro di sostegno alla sorveglianza dello spazio e al tracciamento[27] per collegare in rete queste risorse detenute dagli Stati membri, onde fornire servizi di sorveglianza dello spazio e tracciamento[28] ad utenti identificati (Stati membri, istituzioni dell'UE, proprietari e operatori di veicoli spaziali e autorità di

---

aerea; direttiva 2005/65/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa al miglioramento della sicurezza dei porti; regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, del 31 marzo 2004, relativo al miglioramento della sicurezza delle navi e degli impianti portuali.

[22] Conformemente al diritto dell'UE la Commissione è tenuta a effettuare ispezioni per garantire che gli Stati membri attuino correttamente le prescrizioni relative alla sicurezza aerea e marittima. Ciò include ispezioni presso le autorità competenti degli Stati membri, così come ispezioni negli aeroporti, nei porti, dei vettori aerei, delle navi e dei soggetti responsabili dell'attuazione delle misure di sicurezza. Le ispezioni della Commissione servono a garantire la piena applicazione delle norme UE da parte degli Stati membri.

[23] Regolamento (UE) 2016/4 della Commissione, del 5 gennaio 2016, che modifica il regolamento (CE) n. 216/2008 del Parlamento europeo e del Consiglio per quanto riguarda i requisiti essenziali per la protezione ambientale; regolamento (CE) n. 216/2008, del 20 febbraio 2008, recante regole comuni nel settore dell'aviazione civile e che istituisce un'Agenzia europea per la sicurezza aerea.

[24] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni — Una strategia per l'aviazione in Europa, COM/2015/0598 final del 7.12.2015.

[25] Nel dicembre 2014 il Consiglio ha adottato un piano d'azione per attuare la strategia per la sicurezza marittima dell'Unione europea; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf.

[26] Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo relativa alla strategia e al piano d'azione dell'UE per la gestione dei rischi doganali: affrontare i rischi, rafforzare la sicurezza della catena di approvvigionamento e agevolare gli scambi, COM(2014)527 final.

[27] Si veda la decisione 541/2014 del Parlamento europeo e del Consiglio.

[28] Come allarmi per evitare le collisioni in orbita, allarmi relativi a disgregazioni o collisioni e rientri rischiosi di oggetti spaziali nell'atmosfera terrestre.

protezione civile). Nel contesto dell'imminente strategia spaziale per l'Europa, la Commissione ne esaminerà un ulteriore sviluppo, per monitorare le minacce ibride alle infrastrutture spaziali.

Le comunicazioni satellitari (SatCom) sono risorse fondamentali per la gestione delle crisi, la reazione alle catastrofi, la sorveglianza di polizia, delle frontiere e delle coste. Sono la spina dorsale delle infrastrutture su ampia scala, come i trasporti, lo spazio, o i sistemi aerei a pilotaggio remoto. In linea con l'invito del Consiglio europeo di preparare la prossima generazione di comunicazioni governative via satellite la (GovSatCom), la Commissione, in cooperazione con l'Agenzia europea per la difesa, sta valutando dei modi di raggruppare la domanda, nel contesto dell'imminente strategia spaziale e del piano di azione europeo in materia di difesa.

Per sincronizzare le loro reti (ad es. energia e telecomunicazioni) o per orodatare le operazioni (ad es. mercati finanziari), molte infrastrutture critiche si basano su informazioni con una tempistica precisa. La dipendenza da un unico segnale di sincronizzazione oraria del sistema mondiale di navigazione satellitare non offre la resilienza richiesta per contrastare le minacce ibride. Galileo, sistema globale di navigazione via satellite europeo, offrirebbe una seconda fonte di sincronizzazione affidabile.

***Azione 8* — *Nel contesto dell'imminente 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.***

### 4.2. Capacità di difesa

Per aumentare la resilienza dell'UE alle minacce ibride devono essere rafforzate le capacità di difesa. È importante individuare i settori pertinenti di capacità fondamentali, ad esempio le capacità di vigilanza e riconoscimento. L'Agenzia europea per la difesa potrebbe essere un catalizzatore per lo sviluppo di capacità militari legate alle minacce ibride (ad esempio abbreviando i cicli di sviluppo delle capacità di difesa, investendo in tecnologia, sistemi e prototipi, aprendo il settore della difesa a tecnologie commerciali innovative). Eventuali azioni potrebbero essere esaminate nel quadro dell'imminente piano di azione europeo in materia 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 a tale sviluppo in modo pertinente per l'UE, per lottare specificamente contro le minacce ibride verso uno o più Stati membri.***

### 4.3. Proteggere la salute pubblica e la sicurezza alimentare

La salute dei cittadini potrebbe essere messa in pericolo dalla manipolazione di malattie trasmissibili o dalla contaminazione del cibo, del suolo, dell'aria e dell'acqua potabile con agenti chimici, biologici, radiologici e nucleari (CBRN). Inoltre, la diffusione intenzionale di epizoozie o fitopatie può compromettere seriamente la sicurezza alimentare dell'Unione e avere gravi effetti economici e sociali su settori fondamentali della catena di approvvigionamento dell'UE. Le esistenti strutture europee per la sicurezza sanitaria, la protezione ambientale e la sicurezza alimentare possono essere utilizzate per rispondere alle minacce ibride di questo tipo.

Ai sensi della legislazione dell'UE relativa alle minacce per la salute a carattere transfrontaliero[29], i meccanismi esistenti coordinano la preparazione a tali gravi minacce collegando gli Stati membri, le agenzie dell'UE e i comitati scientifici[30] attraverso il sistema di allarme rapido e di reazione. Il comitato per la sicurezza sanitaria, che coordina le reazioni nazionali alle minacce, può fungere da punto focale sulle vulnerabilità nel settore della salute pubblica[31], per integrare le minacce ibride (in particolare il bioterrorismo) negli orientamenti sulla comunicazione di crisi e negli esercizi di rafforzamento delle capacità (simulazioni di crisi) con gli Stati membri. Nel settore della sicurezza alimentare, attraverso il sistema di allarme rapido per gli alimenti e i mangimi (RASFF) e il sistema comune di gestione dei rischi (CRMS) per le dogane, le autorità competenti si scambiano informazioni sulle analisi del rischio per monitorare i rischi sanitari posti dagli alimenti contaminati. Per quanto riguarda la salute degli animali e delle piante, la revisione in corso del quadro giuridico dell'UE[32] aggiungerà nuovi elementi agli strumenti esistenti[33] ai fini di una migliore preparazione anche alle minacce ibride.

***<u>Azione 10</u> — 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.***

[29] Decisione n. 1082/2013/UE del Parlamento europeo e del Consiglio, del 22 ottobre 2013, relativa alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 2119/98/CE, GU L 293 del 5.11.2013, pag. 1.

[30] Decisione C(2015)5383 della Commissione, del 7 agosto 2015, relativa alla costituzione di comitati scientifici nel settore della sanità pubblica, della sicurezza dei consumatori e dell'ambiente.

[31] In linea con la decisione n. 1082/2013/UE del Parlamento europeo e del Consiglio, del 22 ottobre 2013, relativa alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 2119/98/CE, GU L 293 del 5.11.2013, pag. 1.

[32] Regolamento 2016/429 del Parlamento europeo e del Consiglio relativo alle malattie animali trasmissibili e che modifica e abroga taluni atti in materia di sanità animale ("normativa in materia di sanità animale"), GU L 84 del 31.3.2016. Per quanto riguarda il regolamento del Parlamento europeo e del Consiglio relativo alle misure di protezione contro gli organismi nocivi per le piante ("normativa fitosanitaria"), il Parlamento europeo e il Consiglio hanno raggiunto un accordo politico sul testo il 16 dicembre 2015.

[33] Ad es. banche europee di vaccini, sofisticati sistemi elettronici d'informazione sulle malattie degli animali, maggiori obblighi di misure per i laboratori e altri soggetti che trattano elementi patogeni.

## 4.4. Cibersicurezza

L'Unione europea trae grande vantaggio dalla sua società interconnessa e digitalizzata. Gli attacchi informatici potrebbero bloccare i servizi digitali in tutta l'UE, e gli autori di minacce ibride potrebbero utilizzarli. Per sostenere il mercato unico digitale è importante migliorare la resilienza dei sistemi di comunicazione e informazione in Europa. La strategia dell'Unione europea per la cibersicurezza e l'agenda europea sulla sicurezza forniscono il quadro strategico generale per iniziative europee sulla sicurezza informatica e sulla criminalità informatica. Nell'ambito dei risultati attesi dalla strategia per la cibersicurezza l'UE ha attivamente fatto opera di sensibilizzazione e sviluppato meccanismi di cooperazione e risposte. In particolare, la proposta direttiva sulla sicurezza delle reti e dell'informazione (SRI)[34] affronta i rischi relativi alla sicurezza informatica di un'ampia gamma di fornitori di servizi fondamentali nel settore dell'energia, dei trasporti, della finanza e della sanità. Questi fornitori di servizi, così come i fornitori di servizi digitali essenziali (ad es. cloud computing), dovrebbero prendere adeguate misure di sicurezza e segnalare gli incidenti gravi alle autorità nazionali, annotando ogni caratteristica ibrida. Una volta la direttiva adottata dai colegislatori, l'effettivo recepimento e attuazione dovrebbero favorire le capacità degli Stati membri in materia di cibersicurezza, rafforzando la loro cooperazione nel settore attraverso lo scambio di informazioni e l'applicazione delle migliori prassi nella lotta contro le minacce ibride. In particolare, la direttiva prevede la creazione di una rete di 28 gruppi nazionali di intervento per la sicurezza informatica in caso di incidente (CSIRT) e le CERT-UE[35] per portare avanti la cooperazione operativa su base volontaria.

Per incoraggiare la cooperazione pubblico-privato e gli approcci alla cibersicurezza su scala UE la Commissione ha istituito la piattaforma SRI, che emana orientamenti sulle migliori prassi in materia di gestione del rischio. Mentre gli Stati membri stabiliscono i requisiti di sicurezza e le modalità di comunicazione degli incidenti nazionali, la Commissione incoraggia un elevato livello di convergenza negli approcci alla gestione del rischio, ricorrendo in particolare all'Agenzia UE per la sicurezza delle reti e dell'informazione (ENISA).

***<u>Azione 11</u> — La Commissione incoraggia gli Stati membri, come questione prioritaria, a costituire e utilizzare appieno una rete fra i 28 CSIRT e le CERT-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 SRI per mettere insieme informazioni, competenze e reazioni rapide.***

[34] Proposta della Commissione di direttiva del Parlamento europeo e del Consiglio recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione, COM(2013)48 final — 7/2/2013. Il Consiglio dell'UE e il Parlamento europeo hanno raggiunto un accordo politico su questa proposta di direttiva, che dovrebbe venire formalmente adottata entro breve.
[35] Squadre di pronto intervento informatico (CERT-UE) per le istituzioni dell'UE.

### *4.4.1. Industria*

Il sempre maggiore ricorso al cloud computing e ai big data ha aumentato la vulnerabilità alle minacce ibride. La strategia per il mercato unico digitale prevede un partenariato pubblico-privato contrattuale sulla cibersicurezza[36], che si concentrerà sulla ricerca e l'innovazione e aiuterà l'Unione a mantenere un alto grado di capacità tecnologica in questo settore. Il partenariato pubblico-privato contrattuale servirà a instaurare un clima di fiducia fra i vari operatori di mercato e a sviluppare sinergie fra il versante della domanda e dell'offerta. Se tale partenariato, con le misure di accompagnamento, verterà in primo luogo su prodotti e servizi di cibersicurezza civili, il risultato di queste iniziative dovrebbe permettere agli utilizzatori delle tecnologie di essere maggiormente protetti anche contro le minacce ibride.

***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.***

### *4.4.2. Energia*

La comparsa delle case e degli apparecchi intelligenti e lo sviluppo della rete intelligente, insieme alla sempre maggiore digitalizzazione del sistema energetico, portano anch'essi a una maggiore vulnerabilità agli attacchi informatici. La strategia europea di sicurezza energetica[37] e la strategia dell'Unione dell'energia[38] sostengono un approccio multirischio, in cui sia integrata la resilienza alle minacce ibride. La rete tematica per la protezione delle infrastrutture energetiche critiche promuove la collaborazione fra gli operatori del settore energetico (petrolio, gas, elettricità). La Commissione ha avviato una piattaforma web per analizzare e condividere informazioni sulle minacce e gli incidenti[39] e, per ridurre i punti vulnerabili, sta anche sviluppando insieme alle parti interessate[40] un'ampia strategia del settore energetico sulla cibersicurezza nelle operazioni della rete intelligente. Mentre i mercati dell'energia elettrica sono sempre più integrati, le regole e le procedure su come far fronte alle situazioni di crisi si situano sempre a livello nazionale. Occorre garantire che i governi cooperino fra di loro nella preparazione ai rischi e nella loro prevenzione e attenuazione, e che tutti gli operatori competenti agiscano in base a un insieme comune di norme.

***Azione 13* — *La Commissione emanerà orientamenti destinati ai detentori di risorse della rete intelligente per migliorare la sicurezza informatica 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***

[36] Da avviare a metà 2016.
[37] Comunicazione della Commissione al Parlamento europeo e al Consiglio — Strategia europea di sicurezza energetica — COM/2014/0330 final.
[38] Comunicazione relativa a "Una strategia quadro per un'Unione dell'energia resiliente, corredata da una politica lungimirante in materia di cambiamenti climatici" — COM/2015/080 final.
[39] Centro dell'UE per lo scambio di informazioni sugli incidenti e le minacce — ITIS.
[40] Nella forma di una piattaforma per la cibersicurezza di esperti di energia (EECSP).

***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.***

### *4.4.3. Garantire la solidità dei sistemi finanziari*

Per funzionare, l'economia dell'UE ha bisogno di un sistema finanziario e di pagamento sicuro. Proteggere il sistema finanziario e le sue infrastrutture dagli attacchi informatici, indipendentemente dal movente o dalla natura dell'autore dell'attacco, è un aspetto fondamentale. Per far fronte alle minacce ibride contro i servizi finanziari dell'UE, tale settore deve capire il rischio, deve avere testato le proprie difese e deve disporre della tecnologia necessaria per proteggersi. Analogamente, lo scambio di informazioni sulle minacce fra gli operatori dei mercati finanziari e con le autorità competenti e i principali fornitori di servizi o clienti è essenziale, ma anch'esso deve essere sicuro e deve rispettare le condizioni relative alla protezione dei dati. In linea con i lavori portati avanti nelle sedi internazionali, compresi i lavori del G7 in questo settore, la Commissione si adopererà per individuare i fattori che ostacolano un adeguato scambio di informazioni sulle minacce e proporrà soluzioni. È importante garantire verifiche e miglioramenti regolari dei protocolli per proteggere le attività finanziarie e le pertinenti infrastrutture, compreso un continuo aggiornamento delle tecnologie per il rafforzamento della sicurezza.

***Azione 14 — La Commissione, in cooperazione con l'ENISA[41], con gli Stati membri, con le autorità competenti internazionali, europee e nazionali e con gli istituti finanziari, 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.***

### *4.4.4. Trasporti*

I trasporti moderni (ferroviari, stradali, aerei e marittimi) si basano su sistemi di informazione vulnerabili agli attacchi informatici. Data la dimensione transfrontaliera, l'UE ha un ruolo particolare da svolgere. La Commissione, in coordinamento con gli Stati membri, continuerà ad analizzare le minacce informatiche e i rischi legati alle interferenze illecite con i sistemi di trasporto. La Commissione sta elaborando una tabella di marcia per la sicurezza informatica nell'aviazione in cooperazione con l'Agenzia europea per la sicurezza aerea (AESA)[42]. Le minacce informatiche alla sicurezza marittima sono inoltre affrontate nell'ambito della strategia per la sicurezza marittima dell'Unione europea e del relativo piano d'azione.

***Azione 15 — La Commissione e l'Alto rappresentante (nell'ambito dei loro rispettivi settori di competenza), in coordinamento con gli Stati membri, esamineranno come***

[41] Agenzia UE per la sicurezza delle reti e dell'informazione.

[42] Il nuovo regolamento EASA è attualmente in corso di discussione fra il Parlamento europeo e il Consiglio a seguito della proposta della Commissione del dicembre 2015. Proposta di regolamento del Parlamento europeo e del Consiglio recante regole comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che abroga il regolamento (CE) n. 216/2008 del Parlamento europeo e del Consiglio — COM(2015)613 final, 2015/0277 (COD).

***rispondere in particolare alle minacce ibride relative agli attacchi informatici nel settore dei trasporti.***

### 4.5. Lottare contro il finanziamento delle minacce ibride

Gli autori delle minacce ibride hanno bisogno di finanziamenti per mantenere le loro attività. I finanziamenti possono essere utilizzati per sostenere gruppi terroristici o per appoggiare forme più sottili di destabilizzazione, come il supporto a gruppi di pressione e a partiti politici radicali. L'Unione europea ha intensificato gli sforzi contro il finanziamento della criminalità e del terrorismo, come indicato nell'agenda europea sulla sicurezza e in particolare nel piano d'azione contro il finanziamento del terrorismo[43]. In tale contesto, in particolare, il quadro europeo antiriciclaggio rivisto rafforza la lotta contro il finanziamento del terrorismo e il riciclaggio di denaro e facilita il lavoro delle unità di informazione finanziaria (UIF) per individuare e seguire trasferimenti di denaro e scambi di informazioni sospetti, garantendo al tempo stesso la tracciabilità dei trasferimenti di fondi nell'Unione europea. Potrebbe quindi contribuire a combattere le minacce ibride. Nell'ambito degli strumenti della PESC, ai fini della lotta contro tali minacce potrebbero essere studiate efficaci misure restrittive ad hoc.

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

### 4.6. Rafforzare la resilienza contro la radicalizzazione e l'estremismo violento

Benché gli atti terroristici e l'estremismo violento non siano, *in sé*, di natura ibrida, gli autori di minacce ibride possono interessarsi ai membri vulnerabili della società e reclutarli, facendo opera di radicalizzazione attraverso i moderni canali di comunicazione (compresi i media sociali su Internet e gli intermediari) e la propaganda.

Per combattere i contenuti di carattere estremistico su Internet la Commissione sta analizzando — nell'ambito della strategia per il mercato unico digitale — la necessità di eventuali nuove misure, prestando debita attenzione al loro impatto sui diritti fondamentali alla libertà di espressione e di informazione. Questo potrebbe comportare procedure rigorose per l'eliminazione dei contenuti illegali, evitando al tempo stesso lo smantellamento dei contenuti legali ("notifica e azione"), e maggiore responsabilità e dovere di diligenza da parte degli intermediari nella gestione delle reti e dei sistemi. Tutto ciò andrebbe a completare l'esistente approccio volontario delle imprese di Internet e dei media sociali, che (in particolare in seno al forum dell'UE su Internet), in cooperazione con l'unità UE di Europol addetta alle segnalazioni su Internet, rimuovono rapidamente la propaganda terroristica.

Nel contesto dell'agenda europea sulla sicurezza, la radicalizzazione viene combattuta scambiandosi esperienze e sviluppando migliori prassi, compresa la cooperazione nei paesi terzi. Il gruppo di consulenza per le comunicazioni strategiche per la Siria lavora

[43] Comunicazione della Commissione al Parlamento europeo e al Consiglio relativa a un piano d'azione per rafforzare la lotta contro il finanziamento del terrorismo — (COM(2016)50 final).

per rafforzare l'elaborazione e la diffusione di messaggi alternativi per contrastare la propaganda terroristica. La rete di sensibilizzazione al problema della radicalizzazione aiuta gli Stati membri e gli operatori che devono interagire con individui radicalizzati (compresi i combattenti stranieri) o con persone ritenute vulnerabili alla radicalizzazione. Tale rete organizza attività di formazione e consulenza e offrirà supporto ai paesi terzi prioritari in cui vi sia la volontà di impegnarsi. La Commissione, inoltre, sta promuovendo la cooperazione giudiziaria fra operatori della giustizia penale, compreso Eurojust, per lottare contro il terrorismo e la radicalizzazione negli Stati membri, anche occupandosi dei combattenti stranieri e di coloro che hanno fatto ritorno.

Completando gli approcci di cui sopra nella sua **azione esterna**, l'UE contribuisce a combattere l'estremismo violento anche attraverso l'impegno e le iniziative di sensibilizzazione rivolte all'esterno e la prevenzione (lotta alla radicalizzazione e al finanziamento del terrorismo), così come attraverso misure che affrontino i fattori economici, politici e sociali sottesi che forniscono ai gruppi terroristici l'opportunità di espandersi.

***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.***

### 4.7. Maggiore cooperazione con i paesi tersi

Come sottolineato nell'agenda europea sulla sicurezza, l'UE si concentra maggiormente sul rafforzamento delle capacità nei ***paesi partner*** nel settore della sicurezza, basandosi fra l'altro sulla connessione fra sicurezza e sviluppo e sviluppando la dimensione della sicurezza della politica europea di vicinato riveduta[44]. Queste azioni possono anche sostenere la resilienza dei partner alle attività ibride.

La Commissione intende intensificare ulteriormente lo scambio di informazioni operative e strategiche con i paesi dell'allargamento e nel quadro del partenariato orientale e del vicinato meridionale, se del caso, per contribuire alla lotta contro la criminalità organizzata, il terrorismo, la migrazione irregolare e il traffico di armi di piccolo calibro. Per quanto riguarda l'antiterrorismo, l'Unione europea sta intensificando la cooperazione con i paesi terzi stabilendo dialoghi potenziati in materia di sicurezza e piani d'azione.

Gli strumenti dell'UE per il finanziamento dell'azione esterna servono a predisporre istituzioni funzionanti e responsabili nei paesi terzi[45], presupposto fondamentale per poter reagire efficacemente alle minacce alla sicurezza e per rafforzare la resilienza. In questo

[44] Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni — Riesame della politica europea di vicinato, 18.11.2015, JOIN(2015)50 final.
[45] Idem; comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni — La strategia di allargamento dell'UE, 10.11.2015, COM(2015)611 final; comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni — Potenziare l'impatto della politica di sviluppo dell'Unione europea: un programma di cambiamento, 13.10.2011, COM(2011)637 definitivo.

contesto, la riforma del settore della sicurezza e il rafforzamento delle capacità a sostegno della sicurezza e dello sviluppo[46] sono degli strumenti fondamentali. Nell'ambito dello strumento inteso a contribuire alla stabilità e alla pace[47], la Commissione ha sviluppato azioni per rafforzare la ciberresilienza e la capacità dei partner di individuare e reagire agli attacchi informatici e alla cibercriminalità, che possono servire ai fini della lotta contro le minacce ibride nei paesi terzi. L'UE sta finanziando attività di rafforzamento delle capacità nei paesi partner per attenuare i rischi alla sicurezza legati alle questioni CBRN[48].

Infine, nello spirito dell'approccio globale alla gestione delle crisi, gli Stati membri potrebbero mobilitare gli strumenti e le missioni della politica di sicurezza e di difesa comune (PSDC), in modo indipendente o come complemento agli strumenti dell'UE, per aiutare i partner a rafforzare le loro capacità. Potrebbero essere prese in considerazione le azioni seguenti: i) sostegno alla comunicazione strategica, ii) consulenze per i ministeri chiave esposti alle minacce ibride; iii) sostegno supplementare per la gestione delle frontiere in caso di emergenze. Potrebbero essere esaminate ulteriori sinergie fra gli strumenti della PSDC e gli operatori del settore della sicurezza, delle dogane e della giustizia, comprese le agenzie competenti dell'UE[49], INTERPOL e la Forza di gendarmeria europea, conformemente ai loro mandati.

***<u>Azione 18</u> — 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, in modo indipendente o come complemento agli strumenti dell'UE, per aiutare i partner a consolidare le loro capacità.***

## 5. PREVENZIONE, RISPOSTA ALLE CRISI E RIPRESA

Come indicato al punto 3.1, la proposta cellula dell'UE per l'analisi delle minacce ibride ha il compito di studiare gli indicatori rilevanti per prevenire e reagire a tali minacce e informare i responsabili europei delle decisioni. Se le lacune possono essere compensate da politiche a lungo termine a livello nazionale e dell'UE, a breve termine resta fondamentale rafforzare le capacità degli Stati membri e dell'Unione di prevenire le minacce ibride, reagirvi e riprendersi in modo rapido e coordinato.

[46] Comunicazione congiunta — Potenziare le capacità per promuovere sicurezza e sviluppo — Consentire ai partner di prevenire e gestire le crisi (JOIN(2015)17final).
[47] Regolamento (UE) n. 230/2014 del Parlamento europeo e del Consiglio, dell'11 marzo 2014, che istituisce uno strumento inteso a contribuire alla stabilità e alla pace, GU L 77 del 15.3.2014, pag. 1.
[48] I settori interessati includono la sorveglianza delle frontiere, la gestione delle crisi, il primo soccorso, i traffici illeciti, il controllo delle esportazioni di prodotti a duplice uso, la sorveglianza e il controllo delle malattie, la scienza forense in campo nucleare, la ripresa post-incidente e la protezione delle strutture ad alto rischio. Possono essere condivise con i paesi terzi anche le migliori prassi acquisite grazie agli strumenti sviluppati nel quadro del piano d'azione CBRN dell'UE, come il Centro europeo di formazione per la sicurezza nucleare e la partecipazione dell'UE al gruppo di lavoro internazionale per la sorveglianza delle frontiere.
[49] EUROPOL, FRONTEX, CEPOL, EUROJUST

Una risposta rapida agli eventi provocati dalle minacce ibride è fondamentale. A tale riguardo, la disponibilità di azioni e capacità di protezione civile da parte del centro di coordinamento europeo di risposta alle emergenze[50] potrebbe rappresentare un efficace meccanismo di reazione per gli aspetti delle minacce ibride che richiedono una risposta della protezione civile. Questo potrebbe avvenire in coordinamento con altri meccanismi di risposta e sistemi di allarme rapido dell'UE, in particolare con la sala operativa del SEAE per la dimensione della sicurezza esterna e il centro strategico di analisi e di risposta sulla sicurezza interna.

La clausola di solidarietà (articolo 222 del TFUE) prevede un'azione dell'Unione, così come azioni fra gli Stati membri, se uno Stato membro è oggetto di un attacco terroristico o è colpito da una calamità naturale o provocata dall'uomo. L'azione dell'Unione per assistere lo Stato membro è attuata applicando la decisione 2014/415/UE del Consiglio[51]. Le modalità di coordinamento in seno al Consiglio dovrebbero basarsi sui dispositivi integrati dell'UE per la risposta politica alle crisi[52]. Conformemente a tali modalità, la Commissione e l'Alto rappresentante (nell'ambito dei loro rispettivi settori di competenza) individuano gli strumenti rilevanti dell'Unione e presentano al Consiglio proposte di decisioni su misure straordinarie.

L'articolo 222 del TFUE riguarda anche le situazioni che implicano un'assistenza diretta da parte di uno o più Stati membri a uno Stato membro che abbia subito un attacco terroristico o che sia stato colpito da una calamità. In tali situazioni, la decisione 2014/415/UE del Consiglio non si applica. Data l'ambiguità associata alle minacce ibride, la Commissione e l'Alto rappresentante (nell'ambito dei loro rispettivi settori di competenza) dovrebbero valutare la possibile applicabilità in ultima istanza della clausola di solidarietà nel caso in cui uno Stato membro dell'UE sia oggetto di gravi minacce ibride.

Nel caso in cui molteplici minacce ibride gravi costituiscano un'aggressione armata contro uno Stato membro dell'UE, per apportare una risposta adeguata e tempestiva potrebbe essere invocato, invece dell'articolo 222 del TFUE, l'articolo 42, paragrafo 7, del TUE. L'emergere di minacce ibride gravi e di vasta portata può anche richiedere una maggiore cooperazione e un maggiore coordinamento con la NATO.

Nel preparare le loro forze, gli Stati membri sono incoraggiati a tenere conto delle potenziali minacce ibride. Per essere pronti a prendere decisioni rapide ed efficaci in caso di attacchi ibridi, gli Stati membri devono procedere a esercizi regolari, a livello operativo e politico, per testare la loro capacità decisionale a livello nazionale e multinazionale. L'obiettivo sarebbe quello di disporre di un protocollo operativo comune fra gli Stati membri, la Commissione e l'Alto rappresentante, che definisca efficaci procedure da seguire nel caso di un attacco ibrido, dalla fase iniziale di individuazione

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en
[51] Decisione 2014/415/UE del Consiglio relativa alle modalità di attuazione da parte dell'Unione della clausola di solidarietà, GU L 192 dell'1.7.2014, pag. 53.
[52] http://www.consilium.europa.eu/it/documents-publications/publications/2014/eu-ipcr/

fino alla fase finale d'attacco, e che precisi il ruolo di ciascuna istituzione dell'Unione e di ciascun soggetto in questo processo.

Come elemento importante dell'impegno della PSDC si potrebbe prevedere di organizzare: a) un addestramento civile e militare; b) missioni di tutoraggio e consulenza per migliorare la sicurezza e la capacità di difesa di uno Stato minacciato; c) piani d'emergenza per individuare segnali di minacce ibride e rafforzare le capacità di allarme rapido; d) un sostegno alla gestione dei controlli di frontiera in caso d'emergenza; e) un sostegno in settori specializzati, l'attenuazione dei rischi CBRN e l'evacuazione di non belligeranti.

***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.**

***Azione 20* — La Commissione e l'Alto rappresentante, nell'ambito dei loro 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.**

***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.**

## 6. MAGGIORE COOPERAZIONE CON LA NATO

Le minacce ibride rappresentano una sfida non solo per l'UE ma anche per altre importanti organizzazioni partner, comprese le Nazioni Unite (ONU), l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE), e in particolare la NATO. Una risposta efficace esige dialogo e coordinamento sia a livello politico che operativo fra le organizzazioni. Una più stretta interazione fra l'UE e la NATO renderebbe entrambe le organizzazioni maggiormente in grado di prepararsi e reagire efficacemente alle minacce ibride, in un modo complementare e attraverso un sostegno reciproco, sulla base del principio di inclusione e nel rispetto dell'autonomia decisionale e delle norme sulla protezione dei dati di ciascuna organizzazione.

Le due organizzazioni condividono gli stessi valori e si trovano a dover affrontare sfide simili. Gli Stati membri dell'UE e i membri della NATO si attendono parimenti dalle loro rispettive organizzazioni un aiuto e un intervento rapido, fermo e coordinato in caso di crisi, oppure, idealmente, che si impedisca il verificarsi della crisi. Sono stati individuati una serie di settori in cui prevedere una più stretta cooperazione e un maggiore coordinamento fra l'UE e la NATO, fra cui la consapevolezza situazionale, la comunicazione strategica, la cibersicurezza e la prevenzione e risposta alle crisi. Il dialogo informale in corso fra l'UE e la NATO sulle minacce ibride dovrebbe essere intensificato per sincronizzare le azioni delle due organizzazioni in questo settore.

Per l'elaborazione di risposte complementari UE/NATO, è importante che entrambe le organizzazioni abbiano lo stesso quadro della situazione prima e durante la crisi. Questo potrebbe avvenire grazie a uno scambio regolare di analisi e di esperienze acquisite, ma anche attraverso contatti diretti fra la cellula dell'UE per l'analisi delle minacce ibride e la cellula omologa della NATO. È altrettanto importante rafforzare la conoscenza delle reciproche procedure di gestione delle crisi per garantire reazioni rapide ed efficaci. La resilienza potrebbe venire rafforzata garantendo complementarità fra le norme comuni fissate per le parti critiche delle rispettive infrastrutture, così come una stretta collaborazione nella comunicazione strategica e nella difesa informatica. Esercizi congiunti totalmente inclusivi, sia a livello tecnico che politico, contribuirebbero a rendere più efficaci le rispettive capacità decisionali delle due organizzazioni. Prendere in considerazione ulteriori possibilità di attività di formazione contribuirebbe a sviluppare un livello comparabile di competenza nei settori critici.

***Azione 22* — *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.***

## 7. CONCLUSIONI

La presente comunicazione congiunta presenta azioni volte a contribuire alla lotta contro le minacce ibride e a rafforzare la resilienza a livello nazionale, dell'UE e dei partner. Mettendo l'accento sull'**aumento della consapevolezza e della conoscenza**, viene proposto di istituire specifici meccanismi di scambio di informazioni con gli Stati membri e di coordinare le capacità dell'UE in materia di comunicazione strategica. Vengono delineate 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. In ciascuno di questi settori, l'attuazione delle strategie convenute dall'UE e dagli Stati membri e la piena applicazione, da parte di questi ultimi, della legislazione esistente saranno un primo passo fondamentale, e sono state presentate anche azioni più pratiche per rafforzare ulteriormente questo impegno.

Per quanto riguarda **la prevenzione delle minacce ibride, la risposta e la ripresa**, viene proposto di esaminare la possibilità di applicare la clausola di solidarietà di cui all'articolo 222 del TFUE (come specificato nella corrispondente decisione) e l'articolo 42, paragrafo 7, del TUE in caso di attacchi ibridi gravi e di vasta portata. La capacità decisionale strategica potrebbe essere rafforzata stabilendo un protocollo operativo comune.

Viene proposto infine di **intensificare la cooperazione** e **il coordinamento fra l'UE e la NATO** in un impegno comune di lotta contro le minacce ibride.

Nell'attuare il presente Quadro congiunto l'Alto rappresentante e la Commissione si impegnano a mobilitare i pertinenti strumenti UE a loro disposizione. È importante che l'UE, insieme agli Stati membri, lavori per ridurre i rischi associati all'esposizione a eventuali minacce ibride da parte di entità statali o non statali.