Consiglio
dell'Unione europea

Bruxelles, 18 giugno 2018
(OR. en)

10135/18

HYBRID 9	**ENER 238**
COPS 212	**EUMC 104**
PROCIV 39	**CIVCOM 111**
CSDP/PSDC 334	**TRANS 267**
CYBER 140	**COEST 121**
CFSP/PESC 568	**ESPACE 30**
JAI 646	**COTER 77**
ECOFIN 625	**CSC 194**
POLMIL 83	**IPCR 14**

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	JOIN(2018) 14 final
Oggetto:	RELAZIONE CONGIUNTA AL PARLAMENTO EUROPEO, AL CONSIGLIO EUROPEO E AL CONSIGLIO sull'attuazione del Quadro congiunto per contrastrare le minacce ibride dal luglio 2017 al luglio

Si trasmette in allegato, per le delegazioni, il documento JOIN(2018) 14 final.

All.: JOIN(2018) 14 final

COMMISSIONE
EUROPEA

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

Bruxelles, 13.6.2018
JOIN(2018) 14 final

RELAZIONE CONGIUNTA AL PARLAMENTO EUROPEO, AL CONSIGLIO EUROPEO E AL CONSIGLIO

sull'attuazione del Quadro congiunto per contrastrare le minacce ibride dal luglio 2017 al luglio

INTRODUZIONE

Il documento *Quadro congiunto per contrastare le minacce ibride - La risposta dell'Unione europea*[1] pone al centro delle azioni dell'UE volte a contrastare le minacce ibride la conoscenza situazionale, la resilienza e la risposta. Migliorare la nostra capacità di rilevare e comprendere tempestivamente le attività ibride dolose e consolidare la resilienza delle infrastrutture critiche (ad es. trasporti, comunicazioni, energia, spazio e finanza) delle nostre società e istituzioni sono fondamentali per rafforzare la nostra capacità di resistere agli attacchi e per la ripresa. Per contrastare le minacce ibride sono necessarie azioni sia degli Stati membri sia delle istituzioni europee. La prima relazione sull'attuazione delle 22 azioni individuate nel Quadro congiunto è stata presentata al Consiglio il 19 luglio 2017[2]. Il presente aggiornamento del 2018 presenta una panoramica dei progressi conseguiti dall'estate dell'anno scorso.

Sono stati conseguiti progressi considerevoli in tutte le quattro aree di azione prioritarie:

- migliorare la conoscenza situazionale,
- rafforzare la resilienza,
- rafforzare le capacità degli Stati membri e dell'Unione di prevenire le crisi, reagirvi e riprendersi rapidamente e in modo coordinato,
- rafforzare la cooperazione con la NATO per garantire la complementarità delle misure.

RICONOSCERE LA NATURA IBRIDA DELLE MINACCE

Azione 1: gli Stati membri procedono a uno studio sui rischi ibridi

Per agevolare tale compito il Consiglio ha formato un Gruppo di amici della presidenza, sotto la guida della presidenza di turno. Nel dicembre 2017 gli Stati membri hanno avviato uno studio al fine di valutare le proprie vulnerabilità principali alle minacce ibride. In base alle risposte pervenute dagli Stati membri la presidenza presenterà una relazione al COREPER, presumibilmente entro la fine di giugno 2018.

In considerazione della scadenza del suo mandato alla fine di giugno 2018, durante la riunione di aprile il gruppo ha aperto la discussione sul mandato futuro in base alla proposta della presidenza. La proposta prorogherebbe il mandato attuale fino al 2020, ampliandone la portata; secondo il progetto esistente, il mandato comprenderebbe compiti riguardanti l'analisi delle opzioni per rafforzare la preparazione e la resilienza degli Stati membri, l'osservazione degli sviluppi a livello nazionale e l'assistenza al coordinamento delle politiche nell'ambito delle minacce ibride, l'ausilio al lavoro del Consiglio in merito alla cooperazione UE-NATO per contrastare le minacce ibride, lo scambio di informazioni e l'elaborazione di una concezione comune di tali minacce.

---

[1] JOIN (2016) 18 final.

[2] *Relazione congiunta al Parlamento europeo e al Consiglio sull'attuazione del Quadro congiunto per contrastare le minacce ibride - La risposta dell'Unione europea* [JOIN (2017) 30 final].

ORGANIZZARE LA RISPOSTA DELL'UE: MIGLIORARE LA CONOSCENZA

Azione 2: creazione di una cellula dell'UE per l'analisi delle minacce ibride

La cellula dell'UE per l'analisi delle minacce ibride, istituita all'interno del centro dell'UE di analisi dell'intelligence nel quadro della capacità unica di analisi dell'intelligence in campo civile e militare dell'UE, si avvale di analisti dei servizi di intelligence e di sicurezza degli Stati membri di carattere sia civile che militare e dei loro contributi. Essa ha raggiunto la piena capacità operativa nel luglio 2017 e tale status è stato confermato durante l'esercitazione parallela e coordinata con la NATO del 2017 (PACE 17). La cellula dell'UE per l'analisi delle minacce ibride riceve ed analizza informazioni classificate e pubbliche sulle minacce ibride, provenienti da un'ampia gamma di portatori di interessi. Relazioni ed analisi sono successivamente condivise con le istituzioni dell'UE e gli Stati membri e alimentano il processo decisionale. Ad oggi la cellula dell'UE per l'analisi delle minacce ibride ha prodotto oltre 100 documenti relativi alle minacce ibride. CERT-UE (la squadra di pronto intervento informatico delle istituzioni dell'UE) coadiuva il lavoro della cellula dell'UE per l'analisi delle minacce ibride condividendo le informazioni sulle minacce informatiche emergenti o in essere. Risultano però limitate, al momento, le competenze specifiche nell'ambito delle minacce chimiche, biologiche, radiologiche e nucleari, oltre che informatiche, e dell'attività informativa difensiva.

Al fine di ampliare la propria attività la cellula dell'UE per l'analisi delle minacce ibride ha formato una rete di punti di contatto nazionali. Ad oggi, 26 Stati membri su 28 hanno individuato punti focali che si riuniscono periodicamente per condividere le proprie conoscenze specialistiche con la cellula.

Esiste inoltre una rete equivalente a quella descritta, dedicata specificamente al conseguimento di risultati grazie a varie azioni tese a creare resilienza. Le riunioni sono tenute a cadenza mensile incentrate su questioni tematiche tra cui i trasporti, le infrastrutture, l'energia, la cibersicurezza e le attività di intelligence ostili.

A livello strategico, la cellula dell'UE per l'analisi delle minacce ibride sta costruendo un rapporto con il centro europeo di eccellenza per la lotta contro le minacce ibride a Helsinki, partecipando a seminari, esercitazioni e discussioni regolari su una serie di argomenti al fine di sviluppare competenze utili per contrastare le minacce ibride.

Nel quadro della dichiarazione congiunta sono in corso attività di condivisione quotidiane e congiunte a livello di personale con la sezione della NATO per l'analisi delle minacce ibride. Nel settembre 2017 è stata pubblicata un'innovativa valutazione parallela e coordinata di un tema ibrido, e nel 2018 è prevista la realizzazione di documenti che esamineranno le sfide ibride provenienti dal vicinato meridionale e da quello orientale.

Azione 3: comunicazioni strategiche

Le comunicazioni strategiche hanno ricevuto ulteriore slancio nell'UE, e molti attori diversi stanno sviluppando capacità in questo ambito. La comunicazione *Contrastare la disinformazione online: un approccio europeo*[3] del 26 aprile 2018 riconosce la disinformazione come minaccia ibrida e stabilisce un certo numero di azioni, tra le quali una rete rafforzata tra la Commissione, il Servizio europeo per l'azione esterna e gli Stati membri. Le esperienze positive ottenute dalla task force East StratCom, istituita su mandato del Consiglio europeo nel marzo 2015, vanno sostenute e rafforzate, come proposto nella

[3] COM(2018)236 final.

comunicazione congiunta intitolata *Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride*[4]

L'attività della task force East StratCom è incentrata in gran parte sul sostegno alle delegazioni dell'UE, principalmente nella regione del partenariato orientale e in Russia, e in una certa misura nell'Asia centrale, allo scopo di migliorare la diffusione di messaggi positivi e di raggiungere un maggior numero di destinatari nei paesi o nelle regioni interessati. A sostegno di tali attività la Commissione attua un programma pluriennale di informazione e comunicazione regionale. La task force East StratCom coordina periodicamente le proprie attività anche con gli Stati membri e con la NATO. Oltre a monitorare la disinformazione, la task force East StratCom è attiva nei paesi del partenariato orientale e negli Stati membri per sensibilizzare in merito all'impatto della disinformazione russa. Essa ha anche rafforzato la formazione di personale nei paesi del partenariato orientale al fine di migliorarne le capacità in materia di comunicazioni strategiche e la resilienza alla disinformazione. In futuro è prevista maggiore cooperazione con il quartier generale della NATO e con i centri di eccellenza di Riga e Helsinki, ad esempio la condivisione di analisi e seminari di formazione per giornalisti provenienti dalla regione del partenariato orientale o dalla Russia.

In base alla nuova strategia dell'UE per i Balcani occidentali, è stata istituita una task force dedicata a tale regione per comunicare in modo più efficace le politiche dell'UE a un maggior numero di persone nella regione, e allo stesso tempo per sensibilizzare in merito alle attività di disinformazione mirate ai Balcani occidentali e per contrastarle. La task force e la Commissione hanno stabilito una cooperazione intensa finalizzata a rendere più strategiche e mirate la comunicazione e l'informazione dirette a tale regione, attingendo alle migliori pratiche e concentrandosi sulle campagne informative tematiche. Risulta però scarsa la consapevolezza delle sempre maggiori minacce che prendono di mira specificamente le istituzioni. È necessario costruire una cultura di sensibilizzazione alla sicurezza e sviluppare la capacità delle istituzioni di contrastare le minacce ibride.

La task force di comunicazione strategica per il Sud, istituita nel 2017, ha ricalibrato il proprio mandato per riflettere lo spostamento dell'attenzione dall'antiterrorismo verso un approccio più sfumato mirato al miglioramento delle comunicazioni e dei contatti con il mondo arabo, anche in lingua araba. Considerato che il Daesh o ISIS non è l'unica minaccia in termini di radicalizzazione, tale task force si adopera per ridurre la diffusione di informazioni false sull'UE e della percezione errata di cosa essa sia. A tal fine vengono elaborati, in stretta collaborazione con la Commissione, messaggi positivi sull'Unione europea e sulle sue politiche che permettono di comprendere meglio l'Unione, si realizza una comunicazione più strategica sulle attività dell'Unione nel mondo arabo e si promuovono valori e interessi condivisi. A sostegno di tali attività la Commissione attua un programma pluriennale di informazione e comunicazione regionale.

Azione 4: *centro di eccellenza per la "lotta contro le minacce ibride"*

Il centro europeo di eccellenza per la lotta contro le minacce ibride, istituito nel 2017, costituisce un polo di competenze che coadiuva gli sforzi profusi individualmente e collettivamente dai paesi partecipanti nella lotta contro le minacce ibride mediante la ricerca, la formazione, l'istruzione e le esercitazioni. Il centro è aperto alla partecipazione degli Stati membri dell'UE e dei membri della NATO. Vi hanno aderito recentemente l'Italia, i Paesi Bassi, la Danimarca e la Repubblica ceca, portando il totale dei paesi a 16. ia l'Unione europea sia la NATO sono presenti nel comitato direttivo in qualità di osservatori.

Nel 2018 il centro ha concordato un bilancio e un piano di lavoro, ha elaborato il proprio quadro concettuale e formato tre "comunità di interesse", dedicate rispettivamente all'esercizio

[4] Riferimento da inserire appena noto.

dell'influenza in forme ibride, alle vulnerabilità e alla resilienza, e alla strategia e alla difesa. È stato formato anche un sottogruppo sugli attori non statali che esamina il modo di operare di vari gruppi terroristici e mandatari. Il centro ha pubblicato diverse analisi delle minacce ibride e ospitato numerose riunioni ad alto livello al fine di elaborare una concezione comune delle minacce ibride, condividere le migliori pratiche e cercare risposte comuni nelle comunità dell'UE e della NATO.

ORGANIZZARE LA RISPOSTA DELL'UE: RAFFORZARE LA RESILIENZA

Al fine di rafforzare la resilienza occorre agire in molti settori d'intervento. Le azioni non sono necessariamente specificamente concepite per tenere conto della natura ibrida delle minacce ma possono garantire complessivamente un'UE più resiliente e più preparata a far fronte alle minacce ibride. Per tali motivi, quando rilevante nella descrizione dei progressi conseguiti nell'ambito di ciascuna delle azioni, si inserisce un riferimento al quadro strategico specifico e alle azioni intraprese dall'Unione, in particolare se intraprese nel contesto delle attività finalizzate all'Unione della sicurezza. La presente relazione dovrebbe quindi essere letta unitamente alle relazioni mensili sui progressi compiuti verso la creazione di un'autentica ed efficace Unione della sicurezza, adottate nella stessa data[5].

Azione 5: protezione e resilienza delle infrastrutture critiche

La Commissione ha elaborato un progetto di manuale sugli indicatori di vulnerabilità e sulla resilienza delle infrastrutture critiche dell'UE alle minacce ibride. Il progetto di manuale si trova ora in fase di convalida mediante consultazioni con gli Stati membri. L'adozione della versione definitiva del manuale è prevista nel novembre 2018. Gli indicatori di vulnerabilità saranno inoltre messi alla prova durante l'esercitazione parallela e coordinata con la NATO del 2018 (PACE 18) e da parte di singoli Stati membri che hanno espresso interesse. Un'attenzione particolare andrebbe rivolta allo sviluppo ulteriore di indicatori di rilevazione, volti a facilitare l'allarme rapido all'inizio di attacchi ibridi a infrastrutture critiche. Le minacce ibride saranno inoltre tenute presenti nella prossima valutazione della direttiva europea sulla protezione delle infrastrutture critiche. La Commissione sta anche intensificando il sostegno scientifico per far fronte alle caratteristiche multiple e trasversali delle minacce ibride, concentrandosi in particolare sull'individuazione delle vulnerabilità, sulla rilevazione rapida e sugli indicatori, sulla resilienza, sulla sensibilizzazione e sulle esercitazioni.

Al fine di proteggere risorse essenziali dell'Unione, la Commissione ha inoltre presentato una proposta di regolamento che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione europea, qualora possano incidere sulla sicurezza o sull'ordine pubblico[6]. La proposta della Commissione riguarda gli investimenti diretti, effettuati da persone o imprese di paesi terzi, che possono, tra l'altro, avere effetti sulle infrastrutture critiche (tra cui l'energia, i trasporti, le comunicazioni, l'archiviazione di dati, le infrastrutture spaziali e altre strutture sensibili), sulle tecnologie critiche (tra cui l'intelligenza artificiale, la cibersicurezza, le tecnologie con possibili applicazioni a duplice uso), sulla sicurezza dell'approvvigionamento di fattori produttivi critici, o investimenti che concedano l'accesso a informazioni sensibili o la capacità di controllare informazioni sensibili.

La seconda fase del forum consultivo per l'energia sostenibile nel settore della difesa e della sicurezza (CF SEDSS II) dell'Agenzia europea per la difesa fornirà ulteriore sostegno all'elaborazione del documento concettuale redatto dal gruppo di esperti per la protezione delle infrastrutture energetiche critiche (PCEI), al fine di trasformarlo in un documento

[5] COM(2018) 470 final.

[6] COM(2017) 487 final.

strategico di riferimento a livello di UE. Viene proposto in tal modo un quadro di riferimento per l'individuazione delle migliori pratiche di gestione, ad uso dei ministeri della Difesa, al fine di rafforzare la protezione e la resilienza di tutte le infrastrutture energetiche critiche (CEI) riguardanti la difesa.

<u>Azione 6:</u> ***aumentare la sicurezza dell'approvvigionamento energetico dell'UE e la resilienza delle infrastrutture nucleari***

Dando seguito all'impegno assunto nel settembre 2017 (nella comunicazione congiunta *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*[7]), la Commissione continuerà a sostenere il centro europeo di condivisione e di analisi delle informazioni per l'energia in materia di cibersicurezza.

Al fine di evitare crisi nell'approvvigionamento di gas, gli Stati membri stanno attuando il regolamento sulla sicurezza dell'approvvigionamento di gas adottato l'anno scorso, mentre la Commissione si adopera per facilitare la sua attuazione e la cooperazione tra gli Stati membri all'interno dei gruppi di rischio. Le valutazione comuni del rischio devono essere notificate alla Commissione entro il 1° ottobre 2018. La Commissione riceverà i piani d'azione preventivi e i piani di emergenza entro il 1° marzo 2019. Gli Stati membri dovrebbero concordare bilateralmente modalità di solidarietà entro il 1° dicembre 2018.

Per porre rimedio alla carenza normativa esistente in materia di preparazione ai rischi nel settore dell'energia elettrica sono in corso discussioni su un regolamento specifico che stabilirebbe le regole di valutazione dei rischi, imporrebbe agli Stati membri di redigere piani di preparazione ai rischi comprendenti determinati elementi obbligatori, indicherebbe come gestire le situazioni di crisi e come monitorare la sicurezza dell'approvvigionamento. I piani di preparazione ai rischi dovrebbero anche comprendere accordi di cooperazione regionale, in particolare sulle modalità di gestione di situazioni con crisi simultanee di approvvigionamento dell'energia elettrica. Nell'attuazione del regolamento sulla preparazione ai rischi gli Stati membri dovrebbero redigere i primi piani nazionali di preparazione ai rischi due anni dopo l'entrata in vigore del regolamento. I piani dovrebbero successivamente essere aggiornati ogni tre anni. Il futuro regolamento sulla preparazione ai rischi imporrà inoltre l'esecuzione di esercitazioni periodiche e congiunte tra gli Stati membri per simulare una crisi dell'approvvigionamento dell'energia elettrica. La Commissione ha già avviato la preparazione di tali esercitazioni congiunte con gli Stati membri interessati, il Centro comune di ricerca e il gruppo di coordinamento per l'energia elettrica.

Per quanto riguarda la resilienza delle infrastrutture nucleari, saranno migliorati a breve termine gli scambi di informazioni con e tra gli Stati membri e la Commissione su temi della sicurezza nucleare e si prevede un'analisi per esplorare iniziative supplementari. Sarà eseguita un'analisi del regolamento sulle salvaguardie nucleari e saranno eventualmente elaborati orientamenti per aiutare gli Stati membri a gestire meglio le sorgenti (radioattive) sigillate ad alta attività. A più lungo termine, la Commissione intende rafforzare le attività nel settore nucleare laddove esista un interesse comune degli Stati membri e lo scambio di informazioni e la collaborazione apportino un vantaggio riconosciuto. Essa studierà inoltre le misure opportune per l'attuazione efficace all'interno dell'UE della Convenzione sulla protezione fisica delle materie nucleari e degli impianti nucleari.

Per quanto riguarda il settore della difesa, il forum consultivo per l'energia sostenibile nel settore della difesa e della sicurezza ha preparato una *Roadmap for Sustainable Energy Management in the Defence and Security* (Tabella di marcia per la gestione dell'energia sostenibile nel settore della difesa e della sicurezza) per aiutare il settore della difesa a migliorare la gestione delle infrastrutture energetiche. Il forum consultivo continuerà a

[7] JOIN(2017) 450 final.

vagliare le modalità per consentire al settore della difesa di diventare più efficiente nell'utilizzo delle risorse energetiche, e a esaminare diverse tecnologie al fine di generare progetti potenzialmente utilizzabili dal settore della difesa (ad es. l'energia eolica, l'energia solare, le reti intelligenti, lo stoccaggio di energia, i biocarburanti, le biomasse e la conversione dei rifiuti in energia).

In tale contesto, il programma per l'energia e l'ambiente dell'Agenzia europea per la difesa ha continuato la propria attività tramite il progetto di ricerca "Smart Blue Water Camps" al fine di studiare le possibilità di interventi tecnologici per una gestione sostenibile dell'acqua nei campi militari all'interno dei rispettivi paesi e tramite il contratto di ricerca "Smart Camps Technical demonstrator", che studia la fattibilità dell'integrazione di un'ampia gamma di tecnologie energetiche e ambientali su vasta scala nell'ambiente militare per soddisfare esigenze energetiche, idriche e di gestione dei rifiuti, migliorando allo stesso tempo l'efficacia delle missioni PSDC in termini di costi e militari.

Azione 7: ***sicurezza dei trasporti e della catena di approvvigionamento***

Per tutti i settori dei trasporti, vale a dire l'aviazione civile, il trasporto marittimo e il trasporto terrestre, la Commissione ha intensificato le discussioni con gli Stati membri, l'industria e altri portatori di interessi in merito alle minacce alla sicurezza emergenti di natura ibrida, al fine di acquisire conoscenza e apprendere dall'esperienza.

Nel contesto delle attività di attuazione e della revisione del piano d'azione dell'UE relativo alla strategia per la sicurezza marittima, la Commissione sta analizzando le tendenze nell'ambito della sicurezza marittima (comprese la pirateria e le contese marittime) che potrebbero ripercuotersi sui trasporti e sulle rotte commerciali e incidere sugli interessi dell'UE. Visto che gli Stati membri dell'UE e i paesi membri del SEE controllano oltre il 40% della flotta mercantile mondiale e che l'UE è un importante blocco commerciale, attacchi ibridi alle rotte commerciali marittime avrebbero effetti fortemente destabilizzanti sulle catene del valore e di approvvigionamento in Europa. Dall'analisi dei rischi e dal monitoraggio delle minacce emergenti nel settore marittimo potrebbero scaturire ove opportuno proposte per aggiornare la legislazione specifica in materia di trasporti. Tale attività costituisce altresì la base del lavoro continuo sul miglioramento della conoscenza della situazione marittima, anche nel contesto dello sviluppo dell'ambiente comune per la condivisione delle informazioni (CISE); a tale proposito sono stati selezionati recentemente (all'inizio del 2018), nell'ambito di un nuovo invito a presentare proposte, tre progetti per il miglioramento dell'interoperabilità informatica tra le autorità marittime degli Stati membri.

Con l'adozione del pacchetto sulla guardia di frontiera e costiera[8] nel settembre 2016, il Parlamento europeo e il Consiglio hanno introdotto un articolo comune nei regolamenti istitutivi dell'Agenzia europea della guardia di frontiera e costiera, dell'Agenzia europea di controllo della pesca (EFCA) e dell'Agenzia europea per la sicurezza marittima (EMSA), incaricandole di rafforzare la cooperazione, entro i limiti di ciascun mandato specifico, sia tra loro sia con le autorità nazionali che svolgono funzioni di guardia costiera[9], al fine di aumentare la conoscenza della situazione marittima e di sostenere azioni coerenti ed efficienti in termini di costi. Su tale argomento è stato pubblicato nel 2017 uno studio che individua le

[8] Regolamento (UE) 2016/1624 relativo alla guardia di frontiera e costiera europea.

[9] Le funzioni della guardia costiera sono: 1) sicurezza marittima e gestione del traffico marittimo; 2) incidenti marittimi e servizio di assistenza marittima; 3) ispezione e controllo delle attività di pesca; 4) controllo delle frontiere marittime; 5) protezione dell'ambiente marittimo; 6) prevenzione e soppressione della tratta e del contrabbando e applicazione del pertinente diritto marittimo; 7) ricerca e soccorso in mare; 8) monitoraggio e sorveglianza marittimi; 9) attività doganali marittime; 10) risposta in caso di calamità e incidenti marittimi e 11) sicurezza marittima, in navigazione e nei porti.

componenti comuni e le modalità per aumentare l'interoperabilità e la cooperazione nel campo della valutazione del rischio tra le autorità che svolgono funzioni di guardia costiera[10].

Tra gli argomenti e le minacce emergenti riguardanti i trasporti, anche in relazione ai porti ma non solo, figurano le minacce informatiche alla sicurezza dell'aviazione, il disturbo mediante interferenze e la falsificazione di segnali GPS, le minacce ai satelliti o i problemi nel Grande Nord e nell'Artico. Anche il centro di eccellenza per la lotta contro le minacce ibride di Helsinki partecipa all'analisi di tali minacce ibride riguardanti i trasporti e ha recentemente avviato un'analisi finalizzata alla protezione dei porti.

Le dogane dell'UE hanno un ruolo fondamentale nell'assicurare la sicurezza delle frontiere esterne e della catena di approvvigionamento e in tal modo contribuiscono alla sicurezza dell'Unione europea. La Commissione sta apportando aggiornamenti importanti al sistema di informazioni anticipate sui carichi e di gestione dei rischi doganali, al fine di garantire che le dogane dell'UE ricevano tutte le informazioni necessarie, le condividano in maniera più efficace tra gli Stati membri, applichino le norme comuni e le norme specifiche degli Stati membri in materia di rischio e identifichino più efficacemente le spedizioni ad alto rischio. Nel piano d'azione dell'UE di preparazione ai rischi di natura chimica, biologica, radiologica e nucleare (CBRN)[11] una priorità fondamentale consiste nel garantire la sicurezza delle frontiere e la capacità di individuare importazioni illecite di materiali CBRN. Adattare i sistemi di informazione sui carichi è essenziale per rafforzare il monitoraggio e i controlli in base ai rischi delle catene di approvvigionamento internazionali, affinché non siano introdotti illecitamente nell'UE materiali CBRN. La quindicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza fornisce ulteriori dettagli sulle misure adottate dall'UE per migliorare la preparazione ai rischi CBRN e in particolare sulle azioni intraprese a livello di UE nel quadro del piano d'azione della Commissione per rafforzare la preparazione ai rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare.

Con l'obiettivo di eliminare gli ostacoli alla mobilità militare nell'UE, l'Alto rappresentante e la Commissione hanno presentato il 28 marzo 2018 un piano d'azione per esaminare le possibilità di uso civile e militare della rete transeuropea, semplificare le formalità doganali per i trasporti militari e affrontare i problemi normativi e procedurali riguardanti il trasporto di merci pericolose a fini militari. Nel Quadro finanziario pluriennale la Commissione ha proposto di destinare una dotazione di 6,5 miliardi di EUR al gruppo di politiche della difesa, da eseguire attraverso il meccanismo per collegare l'Europa per sostenere le infrastrutture di trasporto al fine di adattarle alle esigenze della mobilità militare. L'obiettivo è rendere possibile il duplice uso, civile e militare, delle infrastrutture di trasporto.

<u>Azione 8</u>: rafforzare la resilienza dei sistemi spaziali

La proposta della Commissione per l'istituzione del programma spaziale dell'Unione[12] integra gli aspetti della sicurezza, anche in Copernicus e nel quadro di supporto al servizio di comunicazioni satellitari governative e alla sorveglianza dello spazio e al tracciamento, che coprirebbero aspetti della resilienza contro le minacce ibride, in aggiunta alle misure già in atto per Galileo ed EGNOS.

Il quadro di sostegno alla sorveglianza dello spazio e al tracciamento[13] è volto a sostenere la disponibilità a lungo termine delle infrastrutture, dei mezzi e dei servizi spaziali europei e nazionali. Esso ha cominciato a prestare servizi iniziali in materia di prevenzione delle

---

10 https://publications.europa.eu/it/publication-detail/-/publication/217db2fc-15d6-11e7-808e-01aa75ed71a1.

11 COM(2017) 610 final del 18.10.2017.

12 COM(2018) 447 final del 6.6.2018.

13 Decisione n. 541/2014/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, che istituisce un quadro di sostegno alla sorveglianza dello spazio e al tracciamento.

collisioni, frammentazione e rientro incontrollato di oggetti spaziali nell'atmosfera terrestre nel luglio del 2016. I centri operativi nazionali per la sorveglianza dello spazio e il tracciamento e il Centro satellitare dell'UE dispongono di misure di sicurezza dei dati che rispettano le raccomandazioni del Consiglio sugli aspetti relativi alla sicurezza della politica di trattamento dei dati nel quadro della capacità europea di sorveglianza dell'ambiente spaziale[14].

Per quanto riguarda Galileo, la Commissione sta prendendo nuovi provvedimenti per garantire una migliore protezione della fornitura dei dati, elemento essenziale per il buon funzionamento delle infrastrutture critiche che dipendono dalla navigazione satellitare per la misurazione del tempo e la sincronizzazione. È allo studio l'eventuale uso di Galileo per la prestazione di servizi in infrastrutture critiche, quali le reti energetiche, le reti di telecomunicazione e i mercati finanziari. In tale contesto, la proposta di regolamento, formulata dalla Commissione, che istituisce un quadro per il controllo degli investimenti esteri diretti indica i programmi del sistema globale di navigazione satellitare europeo (GNSS) Galileo ed EGNOS come esempi di progetti o programmi di interesse per l'Unione potenzialmente pertinenti nel quadro del controllo degli investimenti esteri diretti a norma del regolamento proposto[15].

L'iniziativa dell'UE in materia di comunicazione satellitare governativa fornirà accesso garantito e sicuro alle comunicazioni satellitari a favore delle missioni, delle operazioni e delle infrastrutture chiave dell'Unione e degli Stati membri. Si tratta di uno strumento importante per contrastare le minacce ibride a varie infrastrutture, anche nei settori dello spazio, dei trasporti e dell'energia.

<u>Azione 9</u>: adattamento delle capacità di difesa rilevanti per l'UE

Il Fondo europeo per la difesa, avviato il 7 giugno 2017, rappresenta un importante passo avanti inteso a incentivare gli sforzi degli Stati membri per aumentare e mantenere la collaborazione in materia di difesa in Europa, al fine di rispondere efficacemente alle sfide strategiche. Attingendo alla sezione "capacità" del Fondo, l'UE integrerà in particolare i finanziamenti nazionali ai progetti collaborativi di sviluppo nel settore della difesa. A tal fine la Commissione ha proposto nel giugno 2017 un regolamento che istituisce il programma europeo di sviluppo del settore industriale della difesa con un bilancio di 500 milioni di EUR per gli anni 2019 e 2020. Un accordo provvisorio sul progetto di regolamento è stato raggiunto il 22 maggio 2018 tra il Parlamento europeo e il Consiglio. Per il prossimo Quadro finanziario pluriennale la Commissione ha proposto un Fondo europeo per la difesa integrato, con una dotazione ambiziosa di 13 miliardi di EUR che prevede oltre 8,90 miliardi di EUR per i progetti collaborativi di sviluppo di capacità nel settore della difesa.L'impatto potenziale della lotta contro le minacce ibride sullo sviluppo delle capacità sarà integrato nel piano riveduto di sviluppo delle capacità che gli Stati membri concorderanno nel giugno 2018.

<u>Azione 10</u>: preparazione sanitaria e meccanismi di coordinamento

La preparazione sanitaria è una componente importantissima della preparazione generale ai rischi CBRN. Per questo motivo la Commissione, nel quadro del suo piano d'azione per rafforzare la preparazione ai rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare, ha preso provvedimenti finalizzati in particolare a condividere in modo efficace le conoscenze.

Di conseguenza la Commissione ha predisposto Chimera, un'esercitazione destinata ai settori della sanità, della protezione civile e della sicurezza in tutta l'UE e nei paesi terzi, al fine di verificare la preparazione e la pianificazione delle risposte nel caso di gravi minacce

[14] Space Situational Awareness Data Policy (14698/12) del 9.10.2012

[15] COM (2017) 487 final, allegato.

transfrontaliere. Lo scenario fittizio dell'esercitazione prevedeva l'emissione deliberata di una malattia trasmissibile, associata ad attacchi informatici a infrastrutture critiche tra cui gli ospedali, in modo da mettere alla prova i meccanismi, i sistemi e gli strumenti di comunicazione esistenti a livello nazionale e dell'UE in risposta a una minaccia ibrida. L'esercitazione a livello dell'UE si è svolta il 30 e 31 gennaio 2018 a Lussemburgo. Ha contribuito a sostenere lo sviluppo intersettoriale di capacità e a migliorare l'interoperabilità e il coordinamento tra i settori della sanità, della protezione civile e della sicurezza a livello dell'UE e degli Stati membri e la collaborazione con i partner internazionali. L'esercitazione ha anche aiutato a individuare le responsabilità attuali e i ruoli di tutti i portatori di interessi nella gestione delle crisi dovute a minacce ibride. È stata verificata l'interazione di sistemi quali il sistema di allarme rapido e di reazione (SARR), il sistema di allarme intersettoriale della Commissione (ARGUS), il sistema comune di comunicazione e di informazione in caso di emergenza (CECIS) e i dispositivi integrati del Consiglio per la risposta politica alle crisi (IPCR). La quindicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza contiene ulteriori dettagli sulle misure dell'UE intese ad aumentare la preparazione ai rischi CBRN.

Nell'aprile 2018 la Commissione ha pubblicato una comunicazione e presentato una proposta di raccomandazione del Consiglio volta a rafforzare la cooperazione nella lotta contro le malattie prevenibili da vaccino, in vista della sua adozione entro la fine del 2018. Il documento punta a combattere la riluttanza alla vaccinazione, migliorare la sostenibilità dei programmi di vaccinazione e aumentare l'efficacia della ricerca e dello sviluppo di vaccini.

Per quel che riguarda un corpo medico europeo, la squadra medica d'emergenza della Norvegia ha ricevuto una classificazione dell'Organizzazione mondiale della sanità (OMS) che ne certifica l'adesione a norme minime di qualità. Nell'aprile 2018 si è tenuta la prima riunione regionale delle squadre mediche d'emergenza della regione europea dell'OMS; la riunione è stata ospitata congiuntamente dalla Commissione, dall'Organizzazione mondiale della sanità e dalle autorità sanitarie del Belgio, paese che presiedeva il gruppo regionale.

Sono attualmente in corso collaborazioni intense tra la European Burns Association (Associazione europea ustioni) e gli Stati membri al fine di elaborare un meccanismo per la gestione di calamità con un alto numero di ustionati. All'inizio dell'ottobre 2018 la Commissione e gli Stati membri terranno un seminario per finalizzare i lavori.

<u>Azione 11</u>: la rete CSIRT (gruppi di intervento per la sicurezza informatica in caso di incidente), CERT-UE e la direttiva NIS

CERT-UE produce documenti di valutazione delle minacce informatiche riguardanti settori critici sia periodicamente sia su base ad hoc. Per diverse modalità di trasporto (trasporti aerei, marittimi e terrestri), la Commissione effettua monitoraggi regolari e si assicura che le iniziative settoriali sulle minacce informatiche siano coerenti con le capacità intersettoriali contemplate dalla direttiva sulla sicurezza delle reti e dei sistemi informativi (la direttiva NIS).

Nel settembre 2017 l'Agenzia europea per la difesa e la presidenza estone del Consiglio dell'UE hanno organizzato una simulazione strategica informatica per i ministri della Difesa dell'UE intitolata CYBRID 17 al fine di sensibilizzare in merito al coordinamento in rapporto agli incidenti informatici a livello politico e agli effetti potenziali delle campagne informatiche offensive. La simulazione era incentrata sulla conoscenza situazionale, sui meccanismi di risposta alle crisi e sulla comunicazione strategica. L'Agenzia europea per la difesa trasferirà elementi di questa simulazione nella piattaforma per l'istruzione, la formazione, la valutazione e le esercitazioni, che sarà istituita a settembre del 2018,

dell'Accademia europea per la sicurezza e la difesa. Esercitazioni analoghe ad alto livello organizzate dalle presidenze dell'UE sono all'esame per il futuro.

Azione 12: ***partenariato contrattuale pubblico-privato sulla cibersicurezza***

La Commissione ha firmato un partenariato pubblico-privato sulla cibersicurezza con l'Organizzazione europea per la cibersicurezza (ECSO) al fine di stimolare le capacità competitive e innovative dell'industria della sicurezza e della privacy digitale in Europa. L'UE investirà in tale partenariato fino a 450 milioni di EUR per proteggere utenti e infrastrutture da attacchi informatici. Si prevede che tale partenariato stimolerà investimenti per un valore di 1,8 miliardi di EUR entro il 2020.

In merito alla sicurezza, nel settembre 2017 la comunicazione congiunta intitolata *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*[16] ha stabilito misure per infondere un forte slancio alle strutture e alle capacità dell'UE in materia di cibersicurezza. L'efficacia della cibersicurezza nell'UE è però ostacolata dalla scarsità di investimenti e coordinamento. L'UE si sta sforzando di porvi rimedio, come indicato nella comunicazione congiunta.

Azione 13: ***resilienza del settore energetico***

Nel giugno 2018 la Commissione stabilirà un flusso di lavoro settoriale per l'energia curato dal gruppo di cooperazione NIS per tenere conto delle particolarità del settore energetico e fornire orientamenti agli Stati membri in merito all'attuazione della direttiva sulla sicurezza delle reti e dei sistemi informativi (la direttiva NIS) per tale settore. In parallelo la Commissione sta lavorando a orientamenti specifici sulla cibersicurezza, che, andando al di là della direttiva NIS, individuano le buone pratiche di cibersicurezza nel settore energetico, destinati agli operatori non contemplati dalla direttiva NIS. La Commissione continuerà a organizzare eventi per lo scambio di informazioni sulle tematiche della cibersicurezza nel settore energetico al fine di sensibilizzare, condividere le buone pratiche, migliorare la cooperazione (oltre le frontiere e tra gestori dei sistemi di trasmissione e gestori dei sistemi di distribuzione), affrontare temi quali le misure fisiche e i nuovi rischi, l'istruzione e le competenze.

Nel lungo termine la Commissione stabilirà un codice di rete contenente regole settoriali specifiche sulla cibersicurezza, come proposto nella rifusione del regolamento sul mercato interno dell'energia elettrica[17] che è attualmente all'esame dei legislatori.

Azione 14: ***resilienza del settore finanziario — piattaforme e reti di scambio di informazioni***

Il piano d'azione per le tecnologie finanziarie della Commissione affronta gli ostacoli che potrebbero limitare la condivisione di informazioni sulle minacce informatiche tra gli operatori dei mercati finanziari e individua soluzioni potenziali per porvi rimedio. Anche la squadra CERT-UE contribuisce alla condivisione di informazioni sugli incidenti.

Azione 15: ***resilienza ad attacchi informatici nel settore dei trasporti***

Proteggere le modalità di trasporto da attacchi informatici è una priorità importante per la Commissione. Nell'aviazione civile si sono compiuti grandi progressi sotto l'aspetto della cibersicurezza, ma non si può mai escludere una vulnerabilità dei sistemi a un guasto tecnico o a una minaccia informatica, come dimostrato dal recente incidente informatico di Eurocontrol che ha riguardato metà dei voli in Europa. La Commissione coopera

[16] JOIN(2017) 450 final.

[17] Proposta di regolamento del Parlamento europeo e del Consiglio sul mercato interno dell'energia elettrica (rifusione), COM(2016) 861 final.

intensamente con l'Agenzia europea per la sicurezza aerea in questo settore. CERT-UE ha firmato un accordo sul livello dei servizi con Eurocontrol e un memorandum di cooperazione con l'Agenzia europea per la sicurezza aerea per aiutare tali organizzazioni e i loro portatori di interessi a gestire le minacce informatiche.

Nel trasporto marittimo l'industria della navigazione ha emesso orientamenti sulla cibersicurezza, successivamente discussi e adottati a livello dell'Organizzazione marittima internazionale, principalmente in una prospettiva mondiale. La cibersicurezza nei porti e nelle strutture portuali europee rimane una delle grandi priorità strategiche, studiata e regolarmente oggetto di discussioni con gli Stati membri, l'industria e i portatori di interessi nel contesto dell'attuazione della direttiva sulla sicurezza delle reti di informazione e del seguito da darvi.

La Commissione intende sviluppare uno strumentario olistico e interattivo per la conoscenza in materia di cibersicurezza che presenti le buone pratiche raccomandate, per aiutare i responsabili della sicurezza e i professionisti del settore dei trasporti a individuare, valutare e mitigare meglio i rischi di cibersicurezza.

Azione 16: ***contrastare il finanziamento del terrorismo***

Nell'ultimo anno la Commissione ha compiuto notevoli sforzi per contrastare il finanziamento del terrorismo, come indicato nelle relazioni periodiche sull'Unione della sicurezza. Recentemente, in occasione del pacchetto sulla sicurezza dell'aprile 2018[18], la Commissione ha adottato ulteriori misure per intensificare la cooperazione tra le autorità competenti per la lotta contro i reati gravi e il terrorismo e per facilitare loro l'accesso alle informazioni finanziarie e l'uso delle medesime, proponendo anche una direttiva[19] per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di reati gravi. Ulteriori particolari sul lavoro svolto recentemente a livello di UE per contrastare il finanziamento del terrorismo sono riportati nella quindicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza.

Al fine di armonizzare le sanzioni per il reato di riciclaggio la Commissione ha presentato una proposta legislativa la cui adozione è prevista per metà del 2018. Nel maggio dell'anno in corso è stata inoltre adottata la quinta direttiva antiriciclaggio al fine di rafforzare un certo numero di misure, come controlli rafforzati per i paesi terzi ad alto rischio, controlli delle piattaforme di cambio di valute virtuali, misure di trasparenza applicabili agli strumenti prepagati, nuovi poteri delle unità di informazione finanziaria e accesso rapido delle stesse unità alle informazioni sui titolari di conti bancari e di conti di pagamento mediante registri centrali o sistemi elettronici di reperimento dei dati.

Azione 17: ***azioni contro la radicalizzazione e analisi della necessità di rafforzare le procedure di eliminazione dei contenuti illegali***

La prevenzione della radicalizzazione violenta, sia nel mondo reale sia in quello virtuale, figura da anni tra le priorità della Commissione. Per incrementare gli sforzi a livello di UE, la Commissione ha formato un gruppo di esperti ad alto livello sulla radicalizzazione, che fornirà raccomandazioni sul coordinamento, sulla sensibilizzazione e sull'impatto delle politiche di prevenzione dell'UE. Il gruppo di esperti ad alto livello sulla radicalizzazione ha consegnato il 18 maggio 2018 la propria relazione finale, che comprende la raccomandazione di istituire un meccanismo di cooperazione dell'UE.

Per quanto riguarda la lotta ai contenuti illegali online, in seguito all'adozione della raccomandazione della Commissione del 1° marzo 2018 l'attenzione si è concentrata sulla riduzione dell'accessibilità di tali contenuti. La Commissione ha avviato una valutazione

[18] COM(2018) 211 final.

[19] COM(2018) 213 final.

d'impatto per determinare se gli sforzi attuali siano sufficienti o se siano necessarie misure supplementari, comprese eventuali misure legislative volte a integrare il quadro normativo esistente, al fine di garantire che i contenuti illegali online siano rilevati e rimossi in modo rapido e proattivo. Il lavoro che la Commissione ha svolto in tale ambito è indicato in maggiore dettaglio nella quindicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza.

Il codice di condotta volto a contrastare l'illecito incitamento all'odio online, sottoscritto da Facebook, Twitter, Google (YouTube) e Microsoft, sta apportando risultati rapidi e positivi. Con il codice di condotta le società si impegnano a compiere progressi significativi per quanto riguarda la verifica celere e la rimozione dei presunti incitamenti illeciti all'odio che sono loro notificati. Il terzo esercizio di monitoraggio della Commissione sull'attuazione del codice, i cui risultati sono stati pubblicati nel gennaio 2018, indica che in media il 70% dei contenuti di incitamento all'odio è rimosso e che le verifiche di tali contenuti sono effettuate entro 24 ore, come prescritto dal codice di condotta. Il codice è diventato una norma per il settore ed è promettente la recente decisione di Instagram e Google+ di aderirvi. Nel marzo 2018 la Commissione ha anche proposto misure supplementari per le piattaforme online, quali la rilevazione automatica, la trasparenza e il feedback agli utenti, oltre a misure di salvaguardia per proteggere la libertà d'espressione[20].

In aggiunta alle azioni già intraprese contro la radicalizzazione e gli incitamenti all'odio online, è opportuno prendere misure per prevenire e mitigare le minacce basate sull'uso di strumenti informatici in contesto elettorale.

<u>Azione 18</u>: maggiore cooperazione con le regioni del vicinato e i paesi terzi

L'Unione europea ha aumentato l'attenzione per il rafforzamento delle capacità e della resilienza nei paesi partner nel settore della sicurezza, anche sviluppando la dimensione della sicurezza della politica europea di vicinato riveduta. Nell'intento di migliorare la capacità dei partner di contrastare le minacce ibride, vengono avviate indagini specifiche sui rischi ibridi al fine di individuare le vulnerabilità critiche e fornire sostegno mirato. Il SEAE, in coordinamento con la Commissione, ha svolto un'indagine con la Repubblica di Moldova. Nel 2018 la Giordania e la Georgia hanno chiesto ufficialmente all'UE di essere sottoposte a indagini sulla loro vulnerabilità, il cui primo passo è adattare il questionario alle esigenze specifiche di tali paesi. Attività complementari sullo sviluppo della capacità in tema di cibersicurezza, in particolare per le infrastrutture critiche, sono state intraprese in Ucraina attraverso le missioni di assistenza tecnica; la Commissione ha inoltre avviato all'inizio del 2018 un nuovo programma esaustivo inteso a migliorare la ciberresilienza dei paesi terzi, specialmente in Africa e in Asia.

L'UE continua a discutere piani e programmi per lo sviluppo delle capacità in materia di sicurezza in ambito nucleare con l'Agenzia internazionale per l'energia atomica e con il governo degli Stati Uniti nel gruppo "Monitoraggio delle frontiere". Il Centro europeo di formazione per la sicurezza nucleare (EUSECTRA) offre formazione sulla prevenzione e la rilevazione nell'ambito della sicurezza nucleare e moduli dedicati alla risposta agli incidenti nucleari. Il piano d'azione della Commissione per rafforzare la preparazione ai rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare comprende azioni specifiche di cooperazione con partner internazionali fondamentali, anche nel contesto della lotta al terrorismo e dei dialoghi sulla sicurezza con paesi terzi interessati.

L'iniziativa sui centri di eccellenza CBRN, finanziata dall'UE, che comprende quasi tutti i partner della politica di vicinato[21], continua ad operare per sviluppare le capacità nazionali e

[20] C (2018) 1177 final.

[21] Con centri di eccellenza CBRN regionali a Rabat, Algeri, Amman e Tbilisi.

regionali dei paesi partner in tema di prevenzione, preparazione e risposta a tali minacce, anche quelle che coinvolgono strutture di sicurezza militare (hard security).

Nelle regioni del vicinato orientale e meridionale, formazione ed esercitazioni di protezione civile sono organizzate nell'ambito dei programmi regionali di prevenzione, preparazione e risposta alle catastrofi naturali e di origine umana (PPRD). La terza fase del programma PPRD Sud è iniziata nel 2018, mentre la seconda fase del PPRD Est finirà nel novembre 2018 (non è esclusa una proroga). Saranno assicurati stretti rapporti con i centri di eccellenza CBRN regionali e con i programmi PPRD Sud ed Est.

PREVENZIONE, RISPOSTA ALLE CRISI E RIPRESA

Se le conseguenze possono essere mitigate da politiche a lungo termine a livello nazionale e di 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, è ora in vigore nell'UE un protocollo operativo che definisce il processo di gestione delle crisi in caso di attacchi ibridi. Continueranno a svolgersi regolarmente attività di monitoraggio ed esercitazioni.

Azione 19: ***un protocollo operativo comune ed esercitazioni per migliorare la capacità decisionale strategica in risposta alle minacce ibride complesse***

Il protocollo operativo comune è stato istituito con un documento di lavoro congiunto del giugno 2016, che costituisce l'orientamento principale per le risposte panistituzionali a una crisi. Nel corso di EUPACE 17 il protocollo è stato messo alla prova in uno scenario ibrido e si è rivelato prezioso come strumento per agevolare l'interconnessione tra i servizi. Ha indicato inoltre i punti di contatto per l'interazione tra i diversi livelli di risposta: politico e strategico, operativo e tecnico, oltre che tra i tre meccanismi principali dell'UE di risposta alle crisi (per le crisi esterne), ARGUS (la piattaforma informatica interna della Commissione per lo scambio di informazioni) e i dispositivi integrati del Consiglio per la risposta politica alle crisi. Il protocollo si è dimostrato prezioso anche durante l'esercitazione parallela CMX17 con la NATO. La prossima esercitazione della serie, PACE 18, avrà luogo nel novembre 2018 e, in base alle lezioni che ne saranno tratte, sarà esaminato il possibile aggiornamento del protocollo.

In settembre e ottobre 2017 l'UE ha effettuato la prima esercitazione parallela e coordinata con la NATO (PACE 17) per mettere alla prova la preparazione e l'interazione tra le due organizzazioni nell'eventualità di una crisi ibrida su larga scala. Nella fase preparatoria hanno avuto luogo scambi intensivi di personale in tutti i quattro ambiti dei manuali tattici ibridi: allarme rapido/conoscenza situazionale; comunicazione strategica; ciberdifesa; prevenzione delle crisi e risposta. L'ampiezza dell'interazione tra il personale dell'UE e della NATO nel corso di EUPACE 17 non ha precedenti. Si è trattato inoltre della prima volta che la NATO ha partecipato ad una tavola rotonda del dispositivo integrato per la risposta politica alle crisi, coordinata dalla presidenza dell'UE; funzionari di alto grado dell'UE hanno partecipato alle discussioni del Consiglio Nord Atlantico. Il processo di apprendimento in base alle lezioni tratte si è concentrato su diversi aspetti, tra i quali l'interazione tra i meccanismi di risposta alle crisi dell'UE e della NATO e le problematiche correlate allo scambio di informazioni classificate tra i servizi delle due organizzazioni, anche in considerazione della necessità di sicurezza delle comunicazioni, in particolare con l'obiettivo di garantire in futuro scambi rapidi e sicuri nel pieno rispetto delle esigenze di controllo del servizio d'origine.

È in corso la programmazione dell'esercitazione coordinata e parallela del 2018, in cui l'UE avrà il ruolo di organizzazione con funzioni guida.

<u>Azione 20</u>: ***esame dell'applicabilità e delle 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'applicabilità della clausola di solidarietà dell'UE e del suo meccanismo di assistenza reciproca, come anche l'interazione di tali disposizioni l'una con l'altra e con i meccanismi di risposta della NATO, tra cui la difesa collettiva prevista dall'articolo 5, è oggetto di ulteriori discussioni e prove nel corso di esercitazioni che prevedono scenari ibridi. Il centro di eccellenza per la lotta contro le minacce ibride di Helsinki ha espresso interesse e disponibilità a portare avanti tale lavoro in termini sia di ricerca sia di esercitazione, contribuendo in tal modo a sviluppare una concezione condivisa tra gli Stati membri e gli Alleati.

<u>Azione 21</u>: ***integrare, utilizzare e coordinare 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 politica estera e di sicurezza comune/politica di sicurezza e di difesa comune e in seguito a un seminario con esperti militari del dicembre 2016 e agli orientamenti del gruppo di lavoro 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 politica di sicurezza e di difesa comune. Tale attività prosegue mediante il piano di sviluppo e attuazione di concetti. In consultazione con il centro europeo di eccellenza per la lotta contro le minacce ibride, lo Stato maggiore dell'UE sta elaborando una concezione sulle modalità con cui le forze armate possono contribuire alla lotta contro le minacce ibride, anche mediante missioni ed operazioni nell'ambito della politica di sicurezza e di difesa comune.

Oltre a ciò, per quanto riguarda l'attività quotidiana lo Stato maggiore dell'UE e gli Stati membri stanno operando per migliorare l'allerta precoce, fornendo l'appoggio dell'intelligence militare alla cellula dell'UE per l'analisi delle minacce ibride. La capacità unica di analisi dell'intelligence coadiuva le task force StratCom del SEAE fornendo consulenze militari al fine di contrastare le campagne di disinformazione che prendono di mira l'UE e singoli Stati membri.

Le capacità militari di contrastare le minacce ibride saranno messe alla prova durante l'esercitazione parallela e coordinata 2018 con la NATO (PACE 18). In base allo scenario ibrido per PACE 18, lo Stato maggiore dell'UE e lo Stato maggiore internazionale della NATO svolgeranno discussioni informali UE-NATO basate sullo scenario, finalizzate a garantire la complementarità nella lotta contro le minacce ibride, qualora le esigenze coincidano, in conformità al principio di inclusività, nel rispetto dell'autonomia decisionale di ogni organizzazione e delle regole sulla protezione dei dati.

COOPERAZIONE UE-NATO

<u>Azione 22:</u> ***cooperazione e coordinamento UE-NATO sulla conoscenza situazionale, la comunicazione strategica, la cibersicurezza e la "prevenzione e risposta alle crisi"***

La lotta contro le minacce ibride rimane un settore importante di interazione tra l'UE e la NATO, in base alla considerazione che, in presenza di una minaccia ibrida, le risorse e le capacità che le due organizzazioni possono mobilitare sono complementari e rafforzano la capacità degli Stati membri e degli Alleati di prevenire tali minacce, fungere da deterrente e darvi risposta. L'esercitazione PACE 17 ha messo alla prova i manuali tattici delle due organizzazioni e quindi la loro capacità di operare insieme in modo rapido ed efficace a sostegno dei paesi membri colpiti. Alla luce dell'esperienza acquisita i due manuali tattici saranno riveduti e aggiornati. Nel settore della comunicazione strategica hanno avuto luogo consultazioni sul sostegno all'Ucraina, alla Bosnia-Erzegovina, alla Repubblica di Moldova e alla Georgia.

Nel settembre 2017 un seminario UE-NATO sulla resilienza ha permesso di riunire esperti di settori strategici critici per scambiare informazioni sulle rispettive attività ed esaminare proposte per proseguire i lavori, in particolare nel campo della protezione delle infrastrutture critiche.

È del 2018 il progetto "Mobilità militare", volto a facilitare gli spostamenti di materiale e personale militare, che potrebbe prendere in considerazione le probabili sfide poste dalle minacce ibride specificamente progettate per rallentare i tempi di reazione degli Stati membri e degli Alleati: si tratta si un settore che si presta ad esercitazioni parallele future e che sarà tenuto presente per EUPACE 19/20.

Il coordinamento delle attività di formazione per la cibersicurezza rappresenta un ambito importante nel quale si potrebbe avere maggiore interazione. La NATO ha anche partecipato in qualità di osservatore alla simulazione "CyberEurope" dell'ENISA nel giugno 2018.

CONCLUSIONI

Migliorare la conoscenza situazionale e rafforzare la resilienza contro le minacce ibride in evoluzione e provenienti da fonti diverse rimangono compiti ardui che impongono sforzi costanti da parte dell'UE. Il quadro congiunto prevede un'ampia gamma di azioni, dal miglioramento della fusione e dello scambio di informazioni al rafforzamento della protezione delle infrastrutture critiche e della cibersicurezza, fino alla costruzione di società resilienti alla radicalizzazione e all'estremismo violento. Il quadro dell'UE per contrastare le minacce ibride ha permesso di fornire sostegno agli Stati membri tramite una serie di misure mirate a irrobustire la capacità dell'UE e degli Stati membri di resistere alle tensioni, di rispondere in modo coordinato agli attacchi nocivi e, infine, di riprendersi.

La risposta dell'UE alle minacce ibride è stata inoltre messa alla prova con successo e utilizzata in diverse esercitazioni congiunte con la NATO e si prevede di procedere nella stessa direzione. Una stretta cooperazione tra tutti gli attori pertinenti nell'UE e nella NATO è la chiave di volta degli sforzi per rafforzare la resilienza. Oltre a ciò, sostenere i paesi partner di vicinato nell'individuazione delle loro vulnerabilità e nel rafforzamento delle loro capacità di lottare contro le minacce ibride contribuisce ad una migliore comprensione della natura delle minacce esterne e apre quindi la strada ad una maggiore sicurezza per il vicinato dell'UE.