Camera dei deputati
XVII LEGISLATURA

DOCUMENTAZIONE PER LE COMMISSIONI
ESAME DI ATTI E DOCUMENTI DELL'UE

26 settembre 2017 **n. 97**

Relazione sull'attuazione del Quadro congiunto per contrastare le minacce ibride (JOIN(2017)30)

Tipo di atto	*Relazione*
Data di adozione	*19 luglio 2017*
Settori di intervento	*Sicurezza europea, politica europea di difesa, lotta contro la criminalità;*
Assegnazione	*25 luglio 2017 - I Commissione affari costituzionali e III Commissione affari esteri*
Segnalazione da parte del Governo	*1° agosto 2017*

FINALITÀ / MOTIVAZIONE

Rafforzare la capacita dell'UE di **contrastare le minacce ibride**.

Per "**minacce ibride**" – nozione per la quale non esiste una definizione sul piano giuridico universalmente accettata – la Commissione europea intende una serie di attività che spesso combinano metodi convenzionali e non convenzionali e che possono essere realizzate in modo coordinato da soggetti statali e non statali pur senza oltrepassare la soglia di guerra formalmente dichiarata. Il loro obiettivo non consiste soltanto nel provocare danni diretti e nello sfruttare le vulnerabilità, ma anche nel destabilizzare le società e creare ambiguità per ostacolare il processo decisionale.

IL CONTESTO

L'UE e il suo vicinato sono chiamati a confrontarsi con **l'aumento delle minacce ibride** che mirano o comunque rischiano di destabilizzare la regione europea e il suo vicinato nel suo complesso.

La **natura transnazionale** di tali **minacce** ha posto la questione di una **azione comune condotta almeno a livello europeo**, volta a **coordinare e supportare l'azione degli Stati membri** ai quali **compete la responsabilità principale** nel contrasto alle minacce ibride.

L'Agenda europea sulla sicurezza presentata dalla Commissione nel **2015** ha affermato specificamente la **necessità di contrastare le minacce ibride** attraverso una maggiore **coerenza** tra le **azioni esterne ed interne** nel settore della sicurezza**.**

La Commissione e l'Alta Rappresentante hanno adottato nell'aprile 2016 **un Quadro congiunto per contrastare le minacce ibride** (*v. oltre*) con il quale sono state individuate **22 azioni** concrete.

Anche la **Strategia globale dell'UE per la politica estera e di sicurezza** presentata dall'Alta rappresentante nel **giugno 2016** considera il **contrasto alle minacce ibride una priorità**, sottolineando di nuovo la necessità di un approccio integrato volto a sviluppare un **quadro integrato** che tenga conto la dimensione della **politica estera**

dell'UE e quella delle **politiche interne dell'UE.**

Infine, a **luglio 2016** i Presidenti del Consiglio europeo e della Commissione europea e il segretario generale della NATO hanno sottoscritto a **Varsavia una dichiarazione congiunta** con l'obiettivo di imprimere un nuovo impulso al **partenariato strategico UE-NATO** e concretizzarlo ulteriormente. La dichiarazione congiunta ha evidenziato sette aree concrete nelle quali la cooperazione tra le due organizzazioni dovrebbe essere potenziata, compresa la **lotta contro le minacce ibride**.

CONTENUTI

La **relazione sullo stato di attuazione del Quadro congiunto per contrastare le minacce ibride** (Join(2017)30) è stata presentata congiuntamente dalla Commissione europea e dall'Alta Rappresentante il **19 luglio 2017**.

IL QUADRO CONGIUNTO PER CONTRASTARE LE MINACCE IBRIDE

Il **Quadro congiunto per contrastare le minacce ibride** (Join(2016)18) è stato presentato il **6 aprile 2016** dalla Commissione europea e dall'Alta rappresentante dell'Unione per gli affari esteri e la politica di sicurezza.

Il Quadro congiunto propone un approccio comune e coordinato, sulla base della premessa che la **responsabilità principale ricade sugli Stati membri**, nella misura in cui la lotta alla minacce ibride attiene alla difesa ed alla sicurezza nazionale.

Il Quadro congiunto individua **quattro aree di azione prioritaria**:

- migliorare la **consapevolezza situazionale**;
- rafforzare la **resilienza** (in particolare per quanto riguarda i **trasporti, le comunicazioni, l'energia, i sistemi finanziari, e le infrastrutture di sicurezza**);
- rafforzare le **capacità degli Stati membri** e dell'Unione di **prevenire** le crisi e **reagire in modo coordinato**;
- rafforzare la **cooperazione con la NATO** per garantire la complementarietà delle misure.

All'interno delle suddette aree di azioni il Quadro congiunto prevede **22 azioni** da condurre a livello di Unione europea e Stati membri.

Si indicano di seguito le **22 azioni del Quadro congiunto** con l'indicazione del loro **stato di attuazione** come riportato dalla relazione sullo stato di attuazione del Quadro congiunto (Join(2017) 30).

Azione 1 - Gli **Stati membri** sono invitati a procedere a uno **studio sui rischi ibridi** per **individuare le vulnerabilità** principali delle **strutture e reti** nazionali e paneuropee.

La relazione sullo stato di attuazione del Quadro congiunto indica che il Consiglio ha istituito un **Gruppo degli amici della presidenza**, gruppo informale con funzioni preparatorie del COREPER che riunisce esperti degli Stati membri, al fine di creare uno **strumento di indagine generale** che li aiuti a individuare i **principali indicatori delle minacce ibride**, a integrarli nei meccanismi di allarme rapido e di valutazione dei rischi esistenti nonché a condividerli ove opportuno. Lo **strumento di indagine** dovrebbe essere **pronto entro la fine del 2017**, in vista dell'inizio delle **indagini che gli Stati membri sono invitati a realizzare al più presto**.

Al riguardo, potrebbe risultare opportuno acquisire elementi informativi e di valutazione da parte del Governo sul lavoro svolto dal Gruppo degli amici della Presidenza anche con riferimento alla esigenza che, nella preparazione dello strumento di analisi e indagine si tenga conto delle specificità, dei rischi e delle vulnerabilità dell'Italia.

Azione 2 - Creazione di una **cellula dell'UE per l'analisi delle minacce ibride.**

La **cellula dell'UE per l'analisi delle minacce ibride** è stata **costituita alla fine del 2016** presso il **centro dell'UE di analisi dell'intelligence**. Le sue analisi sono condivise nell'UE e tra gli Stati membri. Al luglio 2017 sono stati prodotti oltre 50 valutazioni e briefing relativi alle minacce ibride. Dal gennaio 2017 la cellula realizza un bollettino di informazione periodico sulle minacce ibride che analizza le minacce e le problematiche attuali. La cellula dell'UE per l'analisi delle minacce ibride ha, inoltre, all'esame iniziative per potenziare la cooperazione UE-NATO.

Potrebbe risultare opportuno verificare con il Governo quale seguito viene dato alle segnalazioni della cellula per l'analisi delle minacce ibride.

Azione 3 - Aggiornamento e coordinamento delle capacità per la formulazione di **comunicazioni strategiche proattive**.

La relazione sullo stato di attuazione ricorda che l'Alta rappresentante ha istituito la **Task force East StratCom,** che formula previsioni e reagisce alle campagne e ai casi di disinformazione della **Federazione Russa**, migliorando la comunicazione

sulle politiche dell'Unione e rafforzando l'ambiente mediatico nei paesi del vicinato orientale. Negli ultimi due anni la task force ha portato alla luce più di 3.000 casi di disinformazione in 18 lingue. La relazione ricorda, imoltre, il **nuovo sito web www.euvsdisinfo.eu**, inaugurato lo scorso 12 settembre, dotato di uno strumento di ricerca online sulle attività di disinformazione e il progetto il **progetto EU-STRAT** avviato nel maggio del 2016 e finanziato dal programma di ricerca e sviluppo dell'UE Orizzonte 2020, che analizza la politica e i media nei paesi del partenariato orientale. La Commissione europea cofinanzia anche la **Rete europea per la comunicazione strategica**, una rete collaborativa tra Stati membri che condivide analisi, buone pratiche e idee sull'uso delle comunicazioni strategiche nella lotta contro l'estremismo violento e sulla disinformazione.

Azione 4 - Istituzione di un **centro di eccellenza** per la "**lotta contro le minacce ibride**".

La relazione ricorda che nell'aprile 2017 è stato istituito, con sede ad **Helsinki, il Centro europeo per la lotta contro le minacce ibride,** sulla base di una iniziativa congiunta di **10 stati membri dell'UE** (Finlandia, Francia, Germania, Lettonia, Lituania, Polonia, Regno unito, Estonia e Spagna), al quale partecipano anche **Norvegia** e **Stati Uniti.** Tale Centro di eccellenza ha come obiettivi principali quelli di incoraggiare il dialogo a livello strategico in tale ambito e di condurre ricerca e analisi e svolgere attività di formazione ed esercitazioni per migliorare le capacità di contrasto alle minacce ibride.

L'Italia al momento non partecipa a tale iniziativa. Potrebbe in proposito risultare opportuno un chiarimento da parte del Governo sulle ragioni della mancata partecipazione e sull'eventuale intenzione di aderirvi in via successiva.

Azione 5 - Individuazione di strumenti comuni, compresi indicatori, per migliorare la protezione e la **resilienza delle infrastrutture critiche** a fronte delle minacce ibride.

Nel contesto del **Programma europeo per la protezione delle infrastrutture critiche** (EPCIP)[1], la Commissione proseguito i lavori intesi a individuare strumenti comuni, compresi **indicatori di vulnerabilità**, per migliorare la resilienza delle infrastrutture critiche a fronte delle minacce ibride nei settori rilevanti. Nel maggio 2017, nel corso di un seminario sulle minacce ibride alle infrastrutture critiche organizzato la Commissione europea, sono state concordate una **tabella di marcia comune** e azioni da intraprendere per il futuro. La Commissione **consulterà nuovamente le parti interessate in autunno**, con l'obiettivo di trovare un **accordo sugli indicatori entro la fine del 2017**.

L'**Agenzia europea per la difesa** dovrebbe presentare nel corso dell'autunno 2017 un documento volto ad **individuare le lacune in termini di ricerca e capacità comuni** derivanti dalla **connessione tra le infrastrutture energetiche e le capacità di difesa.**

Azione 6 - Diversificare le **fonti di energia** e promuovere norme di sicurezza e protezione per le **infrastrutture nucleari**.

La relazione sullo stato di attuazione ricorda la **proposta di regolamento sulla sicurezza dell'approvvigionamento di gas** (*attualmente ancora all'esame delle istituzioni europee*). La proposta è volta ad assicurare un approccio comune e coordinato a livello regionale alle misure di sicurezza dell'approvvigionamento tra gli Stati membri, prevedendo anche - sulla base del **principio di solidarietà -** che gli Stati membri potranno aiutare i vicini in caso di attacco o crisi grave in modo che le famiglie e le imprese europee non siano colpite da black-out. La relazione ricorda inoltre i progressi compiti in ambito UE nello sviluppo di progetti chiave per **diversificare rotte e fonti energetiche** come i lavori di costruzione nel **corridoio meridionale di trasporto del gas** per tutti i principali progetti di gasdotti: l'espansione del gasdotto del Caucaso meridionale e dei gasdotti transanatolico e transadriatico; l'espansione a monte dello Shah Deniz II e l'espansione del corridoio meridionale di trasporto del gas all'Asia centrale, in particolare al Turkmenistan. La relazione indica, inoltre, che sono in **aumento le importazioni di gas naturale liquefatto** (GNL) in Europa in provenienza **da nuove fonti**, quali gli USA. La relazione ricorda, infine, che il **migliore utilizzo delle fonti energetiche autoctone**, in particolare le fonti rinnovabili, contribuisce alla diversificazione delle rotte e delle fonti energetiche.

Nell'area della **sicurezza nucleare**, la relazione indica la necessità di una attuazione coerente ed efficace delle due **direttive sulla sicurezza nucleare e sulle norme fondamentali di sicurezza**, che gli **Stati membri** sono tenuti a **recepire** entro la fine, rispettivamente, del **2017 e del 2018.**

Azione 7 - Monitoraggio delle minacce emergenti nel settore dei **trasporti**.

[1] L'EPCIP è stato istituito sulla base di conclusioni del Consiglio Ue del 2007 con l'obiettivo generale del miglioramento della protezione delle infrastrutture critiche nell'UE contro tutti i tipi di minacce e pericoli.

In linea con le raccomandazioni della task force europea ad alto livello sulle zone di conflitto[2], la Commissione ha elaborato, con il sostegno di esperti nazionali dei settori dell'aviazione e della sicurezza e del SEAE, una **metodologia di valutazione del rischio comune dell'UE nell'ambito della sicurezza aerea** che consente lo scambio di informazioni riservate e la definizione di un quadro del rischio comune. La Commissione sta vagliando l'espansione delle attività di **valutazione del rischio anche ad altre modalità di trasporto** (ad esempio ferroviario e marittimo) e formulerà **proposte in materia nel 2018**. Nel giugno 2017 la Commissione, il SEAE e gli Stati membri hanno avviato un **esercizio di valutazione del rischio sulla sicurezza ferroviaria** al fine di individuare lacune ed elaborare possibili misure di attenuazione dei rischi.

La Commissione europea, congiuntamente all'Agenzia europea per la sicurezza aerea, sta sviluppando due iniziative intese a rafforzare la cibersicurezza: l'istituzione della **squadra di pronto intervento informatico in materia di aviazione** e la creazione di una **task force per la cibersicurezza nell'ambito dell'impresa comune per la ricerca sulla gestione del traffico aereo nel cielo unico europeo** (SESAR), responsabile per la gestione del traffico aereo nel cielo unico europeo. Nel 2016 l'Agenzia europea per la sicurezza aerea ha condotto analisi delle lacune delle norme vigenti, in particolare attraverso l'istituzione dello *European Centre for Cybersecurity in Aviation* (centro europeo per la cibersicurezza nell'aviazione), che collabora con la squadra di pronto intervento informatico dell'UE (CERT-EU), realizzando analisi delle minacce nell'aviazione, e con EUROCONTROL.

Per quanto concerne le **dogane**, la Commissione intende **potenziare il sistema di informazioni anticipate** sui carichi e di gestione dei rischi doganali al fine di garantire che le dogane dell'UE ottengano tutte le informazioni necessarie dagli operatori per quanto riguarda la circolazione delle merci e siano in grado di **identificare più efficacemente e tempestivamente le spedizioni ad alto rischio**.

Al riguardo si può osservare che allo stato si evidenzia una asimmetria nel livello di controlli e delle misure preventive applicati, rispettivamente, al trasporto aereo e al trasporto ferroviario.

[2] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf.

Azione 8 - Incrementare la resilienza delle **infrastrutture spaziali** contro le minacce ibride.

La Commissione, nel predisporre il quadro normativo relativo alla **comunicazione satellitare governativa (GovSatCom**) e alla sorveglianza dello spazio e al tracciamento nel 2018, integrerà aspetti della resilienza contro le minacce ibride nella sua valutazione (*che dovrebbe essere pronta nell'autunno 2017).* In linea con la strategia spaziale, nel preparare l'evoluzione dei progetti **Galileo e Copernicus** la Commissione valuterà le potenzialità di tali servizi in termini di contributo all'attenuazione della vulnerabilità delle infrastrutture critiche (*la proposta sulla prossima generazione di Galileo e Copernicus è prevista per il 2018*).

Azione 9 - Definizione di progetti relativi alle possibilità di adattamento delle **capacità di difesa specificamente contro le minacce ibride** verso uno o più Stati membri.

Nell'aprile 2017 l'Agenzia europea per la difesa ha completato una relazione di analisi sulle implicazioni militari degli attacchi ibridi alle **infrastrutture critiche dei porti**, che sarà discussa nel corso di un seminario con esperti marittimi nell'ottobre 2017. Un'altra analisi specifica del ruolo del **settore militare nel contesto della lotta contro i mini-droni** è prevista per il 2018. Inoltre nella relazione si indica che le **priorità in termini di capacità individuate dagli Stati membri ai fini del rafforzamento della resilienza contro le minacce ibride** saranno essere **ammissibili al sostegno nell'ambito del Fondo europeo per la difesa** *(la relativa proposta è all'esame delle istituzioni dell'UE si sarà conclusa)* **dal 2019**.

Azione 10 - Aumentare la conoscenza delle minacce ibride e la resilienza nell'ambito degli esistenti meccanismi di preparazione e coordinamento, in particolare del **comitato per la sicurezza sanitaria**.

Al fine di rafforzare la preparazione e la resilienza nei confronti delle minacce ibride, compreso lo **sviluppo di capacità nei sistemi sanitari e alimentari**, la Commissione sostiene gli Stati membri tramite formazione ed **esercizi di simulazione**, favorendo lo scambio di linee guida basate sull'esperienza e finanziando azioni comuni. La Commissione e gli Stati membri stanno preparando **un'azione comune per prevenire e fronteggiare la diffusione transfrontaliera di malattie** anche intervenendo per in materia di **vaccinazione**, comprendente la previsione dell'offerta e della domanda di vaccini e la ricerca sui processi innovativi di fabbricazione al fine di **rafforzare l'offerta di vaccini e migliorare la sicurezza sanitaria a livello dell'UE** (2018-2020).

Azione 11 - Costituire e utilizzare appieno una **rete fra i 28 CSIRT nazionali** (*Computer Security and Incident Response Team*) e la

CERT-UE (squadra di pronto intervento informatico dell'UE).

L'adozione della direttiva ((UE) 2016/1148 sulla sicurezza delle reti e i sistemi informativi ha introdotto le prime norme a livello di UE in materia di cibersicurezza, rafforzando la cooperazione tra gli Stati membri. La direttiva ha infatti istituito la **rete di gruppi di intervento per la sicurezza informatica** in caso di incidente ("CSIRT"), che riunisce tutte le pertinenti parti interessate. Parallelamente la Commissione e la CERT-UE procedono a un monitoraggio delle minacce informatiche e allo **scambio di informazioni con le autorità nazionali**

Al fine di rafforzare gli strumenti per affrontare i ciberattacchi, il **19 settembre 2017** la Commissione europea e l'Alta rappresentante hanno presentato un ulteriore **pacchetto di misure** comprendente:

- l'istituzione di un'**Agenzia dell'UE per la cibersicurezza** che, sulla base dell'esperienza dell'attuale Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), avrebbe il mandato permanente di assistere gli Stati membri nel prevenire i ciberattacchi e rispondere agli stessi in modo efficace. L'agenzia dovrebbe organizzare ogni anno **esercitazioni paneuropee di cibersicurezza** e garantire una migliore **condivisione delle attività d'intelligence sulle minacce** mediante la creazione di centri di condivisione e analisi delle informazioni. L'agenzia contribuirebbe altresì a istituire e attuare il **quadro di certificazione paneuropeo** che la Commissione propone per garantire che i **prodotti e i servizi** che oggi fanno funzionare le infrastrutture critiche (quali le reti energetiche e di trasporto, ma anche di nuovi dispositivi di largo consumo, come ad esempio le automobili connesse) **siano sicuri sotto il profilo cibernetico**;
- l'istituzione di un **centro europeo per la ricerca e le competenze in materia di cibersicurezza** (da creare nel corso del 2018) che, collaborando con gli Stati membri, contribuirà a sviluppare e diffondere gli strumenti e la tecnologia necessari per far fronte alle minacce;
- un **programma** che delinea le **modalità di risposta dell'Europa e degli Stati membri** a livello operativo, in modo rapido e concertato, ai ciberattacchi su vasta scala;
- la creazione di un **Fondo di risposta alle emergenze cibernetiche** che potrebbe fornire un sostegno di emergenza per aiutare gli Stati membri, sul modello di funzionamento del meccanismo di protezione civile dell'UE in caso di incendi o calamità naturali;
- l'**inclusione della ciberdifesa nel quadro della cooperazione strutturata permanente** (PESCO) **e del Fondo europeo per la difesa**.

Azione 12 - Lavorare con l'industria nel contesto di un **partenariato pubblico-privato** sulla **cibersicurezza**, per sviluppare tecnologie volte a proteggere maggiormente gli utenti e le infrastrutture dagli aspetti informatici delle minacce ibride.

Nel luglio 2016 la Commissione, in coordinamento con gli Stati membri, ha firmato con l'industria un **partenariato pubblico-privato sulla cibersicurezza**, che nel quadro del programma di ricerca e innovazione Orizzonte 2020 prevede un investimento fino a **450 milioni di euro** per sviluppare e testare tecnologie volte a proteggere maggiormente gli utenti e le infrastrutture da minacce informatiche e ibride. Il partenariato ha prodotto il **primo programma strategico di ricerca paneuropeo**.

Azione 13 - Definizione di orientamenti destinati ai detentori di risorse della **rete intelligente per migliorare la cibersicurezza dei loro impianti**.

Nel settore dell'**energia** la Commissione sta preparando una **strategia settoriale sulla cibersicurezza** con l'istituzione della piattaforma per la **cibersicurezza degli esperti di energia** per rafforzare l'attuazione della cosiddetta **direttiva NIS** (*Network and Information Security*). La **direttiva (UE) 2016/1148**, adottata nel luglio 2016, stabilisce **misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.** La direttiva, che dovrà essere **recepita negli ordinamenti nazionali entro maggio 2018**, si colloca all'interno di una strategia europea che mira a rafforzare la cybersecurity e la resilienza informatica dell'Unione Europea.

Si ricorda che l'attuazione della direttiva NIS è prevista dalla legge di delegazione europea 2016-2017 (A.C. 4620) attualmente all'esame della Camera.

Per quanto riguarda le **iniziative in corso in Italia**, si ricorda che in attesa dell'attuazione della direttiva direttiva(UE)2016/1148, il **DPCM del 17 febbraio 2017** ha previsto, la redazione di un **piano nazionale per la protezione cibernetica e la sicurezza informatica** (poi pubblicato il 31 maggio 2017 - *v. infra*) e il **rafforzamento del ruolo del CISR** (Comitato Interministeriale per la Sicurezza della Repubblica, presieduto dal presidente del Consiglio) che emanerà direttive con l'obiettivo di innalzare il livello della sicurezza informatica del Paese. Il decreto riconduce il Nucleo sicurezza cibernetica (NSC) all'interno del DIS (Dipartimento delle informazioni per la sicurezza) con il compito di assicurare la risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale in raccordo con tutte le strutture dei ministeri

competenti in materia. È inoltre prevista una forte interazione con l'Agenzia per l'Italia Digitale (AGID) del Dipartimento della Funzione Pubblica, con il ministero dello Sviluppo Economico, con il ministero dell'Interno, con il ministero della Difesa e, infine, con il ministero dell'Economia e Finanze.

Il **piano nazionale per la protezione cibernetica e la sicurezza informatica** mira a:

- potenziare le **capacità di difesa delle infrastrutture critiche nazionali e degli attori** di rilevanza strategica per il sistema Paese;
- migliorare le **capacità tecnologiche, operative e di analisi** degli attori istituzionali interessati;
- incentivare la **cooperazione tra istituzioni ed imprese nazionali**;
- promuovere la **diffusione della cultura della sicurezza cibernetica**;
- rafforzare la **cooperazione internazionale** in materia di sicurezza cibernetica;
- rafforzare le **capacità di contrasto alle attività e contenuti illegali** ***on-line.***

Azione 14 - Promuovere **piattaforme e reti di scambio di informazioni sulle minacce**.

La direttiva (UE) n. 2015/2366 ha introdotto nuove disposizioni per **migliorare la sicurezza degli strumenti di pagamento** e l'autenticazione forte del cliente al fine di **ridurre le frodi**, in particolare nei **pagamenti** ***online***. Attualmente la Commissione, assistita dall'Autorità bancaria europea, e in consultazione con le parti interessate, sta elaborando **norme tecniche di regolamentazione**, che dovrebbero essere pubblicate entro la fine del 2017, in materia di **autenticazione del cliente** nonché di comunicazione comune e sicura per garantire la sicurezza delle operazioni di pagamento. Sul fronte internazionale la Commissione ha inoltre lavorato in stretta cooperazione con i rispettivi partner del G7 alla definizione dei "principi fondamentali del G7 sulla cibersicurezza nel settore finanziario" approvati nell'ottobre 2016.

Nell'ambito del pacchetto di proposte sopra menzionato, presentato il **19 settembre**, la Commissione ha annunciato l'intenzione di presentare nuove proposte in materia di **lotta contro la frode** e la falsificazione di **mezzi di pagamento diversi dai contanti**, **estendendo la portata dei reati** connessi contro i sistemi di informazione a tutte le operazioni di pagamento, comprese le operazioni tramite valute virtuali.

Azione 15 - Promuovere la lotta alle minacce ibride relative agli **attacchi informatici** nel **settore dei trasporti.**

Tale azione dovrebbe esplicitarsi principalmente nell'attuazione del **piano d'azione** relativo alla **strategia per la sicurezza marittima dell'UE**, che dovrebbe promuovere lo scambio di informazioni e un uso di risorse condiviso tra autorità civili e militari.

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

Al riguardo, si segnala che, nel dicembre 2016, la Commissione ha presentato tre proposte legislative, che riguardavano tra l'altro **sanzioni penali** in materia di **riciclaggio di denaro** e di **controlli sul denaro contante** in entrata o in uscita dall'Unione nonché il **congelamento e la confisca dei beni**.

Tutti gli Stati membri erano inoltre tenuti a recepire entro il 26 giugno 2017 la quarta **direttiva antiriciclaggio** (che l'Italia ha recepito con il d. lgs 25 maggio 2017, n. 90) tale direttiva:

- rafforza l'**obbligo di valutazione del rischio per banche, avvocati e contabili**;
- elabora chiari requisiti di trasparenza per le **imprese** riguardo la **titolarità effettiva**. Queste informazioni saranno inserite in un **registro centrale** a disposizione delle autorità nazionali e dei soggetti obbligati;
- semplifica la **cooperazione e lo scambio di informazioni** tra le unità di informazione finanziaria di diversi Stati membri per individuare e seguire trasferimenti di denaro sospetti;
- **rafforza i poteri sanzionatori** delle autorità competenti.

Nel luglio 2016 la Commissione ha adottato una **proposta** (COM(2016)450, attualmente all'esame del Parlamento europeo e del Consiglio dell'UE) volta a irrobustire ulteriormente le norme dell'UE in **materia di antiriciclaggio**:

- aumentando la trasparenza sui veri **titolari di società e** ***trust***;
- ampliando la gamma di informazioni a disposizione delle unità di informazione finanziaria, che avranno accesso ai registri centralizzati dei conti bancari e dei conti di pagamento;
- **includendo** nell'ambito di applicazione della direttiva antiriciclaggio **piattaforme di scambio di valute virtuali** e prestatori di servizi di portafoglio digitale.

Azione 17 - Rafforzare le procedure di eliminazione dei **contenuti illegali da Internet**.

La Commissione sta proseguendo **l'attuazione strategia di risposta alla radicalizzazione** definita dalla comunicazione "Sostenere la prevenzione della radicalizzazione che porta all'estremismo violento" del giugno 2016. La strategia stabilisce **azioni chiave**, quali la **promozione** di un**'istruzione inclusiva e di valori comuni**, il **contrasto della propaganda estremistica online**

e della **radicalizzazione nelle carceri**, l'intensificazione della **cooperazione con paesi terzi**.

Conformemente all'Agenda europea sulla sicurezza, la Commissione ha preso provvedimenti per **ridurre la disponibilità di contenuti illegali online**, in particolare mediante l'**unità UE addetta alle segnalazioni su Internet di Europol** e il **Forum dell'UE su Internet**. Sono stati compiuti progressi significativi anche nel quadro del **codice di condotta volto a contrastare l'illecito incitamento all'odio online**.

Le **piattaforme online** svolgono un ruolo determinante nell'affrontare i contenuti illegali o potenzialmente dannosi. Nell'ambito della **strategia per il mercato unico digitale**, la Commissione intende garantire un **migliore coordinamento dei dialoghi con le piattaforme incentrati** sui meccanismi e sulle soluzioni tecniche in materia di rimozione dei contenuti illegali. La Commissione fornirà inoltre orientamenti sulle norme in materia di responsabilità.

Il **17 luglio 2017** il Forum dell'UE su Internet ha presentato un **piano d'azione per contrastare i contenuti di stampo terroristico online**. Tale piano comprende misure volte a incrementare la rilevazione automatica dei contenuti illeciti di stampo terroristico online.

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

La Commissione europea ha avviato, come **progetto pilota**, uno **studio sui rischi** in cooperazione con la **Repubblica di Moldova**. Lo studio ha l'obiettivo di contribuire a individuare le principali vulnerabilità del paese e ad assicurare che l'assistenza dell'UE sia destinata specificamente a tali settori. La Commissione intende **avviare iniziative analoghe a favore di altri paesi vicini**, seppur con adattamenti mirati per tenere conto delle diverse situazioni nazionali locali e di minacce specifiche e per evitare sovrapposizioni con i dialoghi in corso in materia di sicurezza e di contrasto al terrorismo.

Più in generale, il 7 luglio 2017 la **Commissione e l'Alta rappresentante** hanno adottato una **comunicazione congiunta** su "**Un approccio strategico alla resilienza nell'azione esterna dell'UE**" JOIN (2017) 21. L'obiettivo è quello di sostenere i paesi partner a diventare più resilienti alle attuali sfide globali. La comunicazione riconosce la necessità di **abbandonare gli obiettivi di contenimento delle crisi** per **orientarsi verso un approccio alle vulnerabilità più strutturale e di lungo termine**, focalizzato sulla previsione, sulla prevenzione e sulla preparazione.

Azione 19 - Definizione di un **protocollo operativo comune e esercizi regolari** per migliorare la capacità decisionale strategica in risposta alle minacce ibride.

In attuazione di tale azione, la Commissione europea e l'Alta Rappresentante hanno presentato il **5 luglio 2016** un **protocollo (EU-Playbook)** che individua le **modalità operative** che l'UE intende attivare in **caso di minacce ibride**. Il protocollo, in attuazione dell'azione 19 del quadro congiunto, indica le procedure che verranno seguite a livello l'UE, dalla fase iniziale di identificazione della minaccia a quella finale di un eventuale attacco, volte a garantire un **migliore coordinamento delle azioni di contrasto alle minacce ibride, tra i vari livelli decisionali, operativi e tecnici** e con **partner esterni**, in particolare in ambito **NATO**.

Azione 20 - Esame dell'**applicabilità** dell'**articolo 42, paragrafo 7** del TUE (obbligo di prestare aiuto e assistenza in caso di aggressione armata ad altro Stato membro dell'UE) e dell'**articolo 222 del TFUE** (**clausola di solidarietà**), in caso di attacchi ibridi gravi e di vasta portata.

L'**articolo 42, paragrafo 7,** del TUE prevede che qualora uno Stato membro subisca una aggressione armata nel suo terriotrio, gli altri Stati membri sono tenuti a prestargli aiuto ed assistenza con tutti i mezzi in loro posseso, in conformita dell'articolo 51 della Carta delle Nazioni Unite. disposizioni in caso di aggressione armata nel territorio di uno Stato membro. L'**articolo 222 del TFUE** prevede disposizioni (clausola di solidarietà) applicabili se uno Stato membro è oggetto di un attacco terroristico o è colpito da una calamità naturale o provocata dall'uomo**. In caso di attacchi ibridi**, che sono una combinazione di azioni criminali e sovversive, nella relazione si indica che è **più probabile il ricorso all'articolo 222**, secondo le modalità di attuazione previste dalla decisione 2014/415/UE del Consiglio. In caso di un **attacco ibrido che comprenda un'aggressione armata**, potrebbe, invece, essere invocato l'**articolo 42, paragrafo 7**.

Azione 21 - L'**Alta rappresentante**, **coordinerà le capacità di azione militare nella lotta contro le minacce ibride** nell'ambito della politica di sicurezza e di difesa comune.

In risposta al compito di integrare le capacità militari per sostenere la PESC/PSDC e in seguito a un seminario con esperti militari del dicembre 2016 e agli orientamenti del gruppo del comitato militare dell'Unione europea nel maggio 2017, l'11 **luglio 2017 il Comitato militare dell'UE** ha presentato **il parere sul contributo militare dell'UE alla lotta contro le minacce ibride nell'ambito della PSDC**, nel quale si sottolinea la necessità di una più

forte cooperazione tra i servizi di intelligence militare e la cellula dell'UE per l'analisi delle minacce ibride; promuovere supporto militare alle task forces STRATCOM; rivedere le procedure di gestione delle crisi e generazione della forza alla luce dei rischi posti dalla minacce ibride; rafforzare la cooperazione con le strutture NATO che si occupano di minacce ibride.

Azione 22 - Rafforzare la **cooperazione** e il coordinamento con la **NATO**.

La **lotta alle minacce ibride** è **uno dei sette settori** di cooperazione individuati nella **dichiarazione congiunta sul rafforzamento della cooperazione tra UE e NATO** firmata l'8 luglio 2016 a **Varsavia**, che prevede 42 proposte di attuazione. Molte delle azioni specifiche intese a contrastare le minacce ibride sono già state menzionate, tra cui il centro europeo di eccellenza per la lotta contro le minacce ibride, una migliore consapevolezza situazionale, l'istituzione della cellula dell'UE per l'analisi delle minacce ibride e la sua interazione con la nuova sezione della NATO per l'analisi delle minacce ibride, così come la collaborazione tra i gruppi per la comunicazione strategica. Per la prima volta, il personale della NATO e quello dell'UE effettueranno esercitazioni congiunte su come rispondere a uno scenario ibrido.

ESAME PRESSO LE ISTITUZIONI DELL'UE

La relazione è stata **assegnata alla Commissione Affari esteri del Parlamento europeo**, che non ha ancora avviato l'esame.

ESAME PRESSO ALTRI PARLAMENTI NAZIONALI

Sulla base dei dati forniti dal sito IPEX, l'esame dell'atto risulta **in corso** presso il **Parlamento svedese** e il **Consiglio nazionale della Repubblica slovacca**.