COMMISSIONI RIUNITE

I (Affari costituzionali, della Presidenza del Consiglio e interni) e III (Affari esteri e comunitari)

S O M M A R I O

ATTI DELL'UNIONE EUROPEA:

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
(Esame, ai sensi dell'articolo 127, comma 1, del Regolamento, e rinvio) 3

UFFICIO DI PRESIDENZA INTEGRATO DAI RAPPRESENTANTI DEI GRUPPI 12

ATTI DELL'UNIONE EUROPEA

Martedì 17 ottobre 2017. — Presidenza del vicepresidente della III Commissione, Andrea MANCIULLI.

La seduta comincia alle 13.30.

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.

(Esame, ai sensi dell'articolo 127, comma 1, del Regolamento, e rinvio).

Le Commissioni iniziano l'esame del provvedimento in oggetto.

Andrea MANCIULLI, *presidente*, ricorda che l'atto è stato trasmesso dalla Commissione europea il 24 luglio 2017 in attuazione del Protocollo sul ruolo dei Parlamenti nazionali allegato al Trattato sull'Unione europea e che lo stesso provvedimento è assegnato alla XIV Commissione per l'espressione del parere. Ricorda, altresì, che a conclusione dell'esame le Commissioni potranno adottare un documento finale per esporre il proprio avviso su possibili iniziative da assumere.

Anche alla luce del suo impegno in qualità di presidente della delegazione italiana presso l'Assemblea parlamentare della NATO, segnala la particolare rilevanza e attualità del provvedimento, che fa il punto sulle iniziative adottate dall'Unione europea in vari settori per contrastare le cosiddette minacce ibride definite dal Quadro congiunto presentato dalla Commissione europea e dall'Alta Rappresentante per gli affari esteri e la politica di sicurezza nell'aprile 2016, offrendo agli Stati membri specifiche indicazioni per azioni e iniziative.

Cristian INVERNIZZI, *vicepresidente della I Commissione*, in sostituzione del presidente Mazziotti di Celso, relatore per la I Commissione sul provvedimento in titolo, impossibilitato a partecipare alla seduta, fa presente che nella sua relazione illustrerà i progressi realizzati nell'attuazione del Quadro congiunto e gli obiettivi delle ulteriori misure che si intendono presentare per contrastare le cosiddette

minacce ibride. Rileva infatti che, in assenza di una definizione giuridicamente vincolante o comunque largamente condivisa, la Commissione europea intende per minacce ibride le attività che quasi sempre combinano metodi convenzionali e non convenzionali e, che possono essere realizzate in modo coordinato da soggetti diversi dalle entità statuali. Il loro obiettivo non consiste soltanto nel provocare danni diretti, approfittando delle vulnerabilità degli Stati e delle comunità che ne sono vittime, ma anche di provocare destabilizzazioni. In sostanza, ci si trova in presenza di un fenomeno che presenta notevoli elementi di novità, non essendo riscontrabile negli scenari internazionali fino a qualche anno fa e che si caratterizza per la difficile prevedibilità sia nei tempi in cui tali minacce possono essere tradotte in comportamenti lesivi concreti, così come nelle modalità, per quanto concerne i mezzi impiegati, e nei danni che ne possono derivarne. La natura transnazionale di tali minacce ha imposto, inevitabilmente, la necessità di individuare strategie di prevenzione e contrasto comuni, 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. In tal senso, sia l'Agenda europea sulla sicurezza, presentata dalla Commissione nel 2015, sia la Strategia globale dell'Unione europea per la politica estera e di sicurezza, presentata dall'Alta rappresentante nel giugno 2016, hanno sottolineato la necessità di un approccio integrato volto a sviluppare un quadro integrato che tenga conto della dimensione della politica estera dell'Unione europea e quella delle politiche interne dell'Unione medesima.

Osserva che 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.

Segnala in primo luogo, con riferimento ai profili che incidono prevalentemente sulla sicurezza interna, che tutti gli elementi informativi forniti nella relazione si riferiscono a iniziative adottate prevalentemente a livello europeo o comunque su un piano di collaborazione transnazionale. Ciononostante, quelle iniziative chiamano direttamente in causa i governi nazionali dei singoli Paesi ai quali spetta in prima battuta assicurare ai rispettivi cittadini condizioni accettabili di sicurezza. In sostanza, l'esigenza imprescindibile di un'azione condivisa a livello almeno europeo, fermo restando che su questa materia è comunque indispensabile una fattiva collaborazione anche con i maggiori *partner* extraeuropei, a partire dai Paesi membri della NATO, non può intendersi nel senso che i singoli Paesi membri sono esentati dall'obbligo di compiere il massimo sforzo possibile per aggiornare strategie e strumenti di intervento per prevenire e contrastare le minacce ibride. Si tratta, evidentemente, di un compito non semplice proprio per il carattere originale e per molti versi imprevedibile che contraddistingue il fenomeno. È evidente che la definizione di strategie efficaci a livello nazionale può comportare cambiamenti anche radicali negli assetti organizzativi e nelle prassi operative dei soggetti preposti a gestire la materia della sicurezza interna. Sarebbe quindi opportuno che sulle singole azioni, individuate nella relazione nel numero complessivo di 22, il Governo fornisca utili elementi informativi e di valutazione. Ciò vale in primo luogo per le iniziative assunte da alcuni Paesi membri ovvero all'Unione europea, alle quali l'Italia non ha ritenuto di partecipare ovvero non ha ancora dato puntuale seguito: in questi casi occorre chiarire le ragioni per la mancata partecipazione o dei ritardi o degli eventuali impedimenti fin qui emersi. D'altra parte, anche sulle questioni estremamente delicate che investono la sicurezza delle reti e dei trasporti potrebbe risultare opportuno

fare il punto della situazione per chiarire quali iniziative sono state assunte o sono in procinto di essere adottate a livello nazionale per consentire ai cittadini di utilizzare le infrastrutture per la mobilità nelle condizioni di maggiore sicurezza possibile. A questo proposito occorre certamente rimediare quanto prima al divario che si registra nel livello di sicurezza nei controlli tra il traffico aereo e il traffico ferroviario. Più avanzati sembrano i progressi avviati a livello interno per quanto concerne il tema della cibersicurezza e delle reti informatiche. Anche in questo caso, tuttavia, occorre chiarire se alle previsioni normative, recentemente adottate, stanno facendo seguito azioni concrete. In sostanza, siamo in presenza di un documento estremamente complesso che va apprezzato per lo sforzo si fornire un quadro trasversale complessivo delle azioni intraprese e di quelle da avviare nei diversi settori che possono essere interessati. Dobbiamo tuttavia essere consapevoli che trattandosi di un tema che si caratterizza per una marcata originalità, non è facile trovare le risposte più adeguate e i rimedi più efficaci.

Paolo ALLI (AP-CpE-NCD), *relatore per la III Commissione*, esprimendo soddisfazione per l'avvio dell'esame di un provvedimento tanto importante sul tema delle minacce ibride – di cui si occupa da tempo non solo in qualità di componente della III Commissione ma anche grazie all'esperienza straordinaria, che condivide con il presidente Manciulli, in sede di Assemblea parlamentare della NATO, che ha l'onore di presiedere – ricorda la nota affermazione del generale prussiano Karl Von Clausewitz secondo cui « la guerra non è altro che la pura continuazione della politica con altri mezzi ». Il generale Von Clausewicz aveva già allora intuito che tra gli « altri mezzi » dei conflitti rientrano, oltre allo strumento militare, strumenti di tipo ibrido il cui utilizzo, in tempi moderni, è stato riscontrato già in occasione dei conflitti in Libano, Afghanistan o Iraq. Tuttavia l'evento che ha portato alla ribalta la guerra ibrida è certamente il conflitto tra Federazione Russa e Ucraina, segnato dall'annessione della Crimea e dall'appoggio di Mosca alla minoranza russa in rivolta nel Donbass. Richiama, inoltre, la definizione di minaccia ibrida data dallo studioso statunitense Russell Glenn secondo cui per minaccia ibride si deve intendere « qualsiasi avversario che simultaneamente e in modo mirato utilizzi una combinazione di strumenti politici, militari, economici, sociali e informativi, di metodi tradizionali e non, ad impatto catastrofico o di terrorismo e di distruzione criminale. Può includere una combinazione di attori statali e non ». Ricorda, inoltre, un documento elaborato dalla NATO nel 2014, intitolato « *Guerra ibrida, risposta ibrida* ? », in cui si analizzano le possibili risposte a eventuali minacce ibride.

Associandosi alla relazione illustrata dall'onorevole Invernizzi, svolge alcune considerazioni introduttive sulle sfide alla sicurezza che l'Unione europea e gli Stati membri affrontano ormai da più di vent'anni, da quando cioè con la fine del bipolarismo, da un lato, e con l'attentato alle Torri Gemelle, dall'altro, sono cambiate le categorie di fondo nel linguaggio internazionale e nella percezione collettiva della sicurezza e si è innescata una dinamica crescente nella qualità delle minacce, sempre meno convenzionali.

Sottolineando come gli strumenti della guerra ibrida siano sostanzialmente la propaganda, la disinformazione, il terrorismo, le leve economiche, gli attacchi informatici e gli attacchi alle strutture sensibili, sostiene che si assiste ad un'evoluzione verso terrorismi che ricorrono allo spazio digitale per sferrare complessi attacchi informatici o come strumento di influenza collettiva, con campagne di disinformazione e manipolazione dei media, nell'intento di indebolire Stati, apparati complessi e, al fondo, mettere a repentaglio libertà e diritti. Ritiene che tutto ciò evidenzi un dato che rappresenta la sfida di fondo, vale a dire la vulnerabilità delle società e delle istituzioni democratiche, nate per corrispondere all'obiettivo della convivenza pacifica, non a quello di uno

stato di guerra permanente. Crede, dunque, che sia la resilienza globale la nuova frontiera di impegno comune, cui è dedicato il documento in esame, riferito all'attuazione del Quadro congiunto per contrastare le minacce ibride adottato nel 2016.

Specifica che il motivo per cui le Commissioni I e III si occupano di tale tema è legato al fatto che, sebbene l'UE possa e debba assistere gli Stati membri nel consolidamento della loro resilienza nei confronti delle minacce ibride, la responsabilità principale ricade sugli Stati membri, nella misura in cui la lotta contro le minacce ibride attiene alla difesa e alla sicurezza nazionale. D'altra parte, ricorda che l'Unione europea ha abbracciato un approccio globale più integrato alla sicurezza e alla difesa e che, dunque, la lotta alle minacce ibride rientra tra i compiti di un « un'Europa che protegge », evocata dal presidente Juncker nel discorso sullo stato dell'Unione del settembre 2016. Ricorda che questi temi sono anche stati oggetto del dibattito sul futuro dell'Europa, come riconosciuto nella Dichiarazione di Roma del 25 marzo 2017, come pure della dichiarazione congiunta sul partenariato strategico UE-NATO siglata a Varsavia nel 2016.

Infine, ritiene che un ulteriore elemento che va tenuto nel debito conto, anche in considerazione del contesto politico europeo, testimoniato dall'andamento delle consultazioni elettorali nei singoli Stati membri, sia che l'Europa deve necessariamente diventare il garante della nostra sicurezza in quanto nessuno Stato membro può affrontare da solo le sfide alla sicurezza, ancor meno se di tipo ibrido. La cooperazione in materia di difesa e di sicurezza non è quindi una possibilità ma una necessità. Segnala che, come affermato nell'Agenda europea della sicurezza presentata dalla Commissione nel 2015, la necessaria azione comune si basa sulla necessità di una maggiore coerenza tra le azioni esterne ed interne nel settore della sicurezza. Il tema delle minacce ibride è stato riconosciuto come una priorità anche nella Strategia globale dell'UE per la politica estera e di sicurezza, che ha sottolineato la necessità di integrare la dimensione della politica estera dell'Unione e quella delle politiche interne. Indubbiamente la collaborazione tra le *intelligence* e i sistemi di sicurezza nazionali resta lo strumento più efficace e su cui occorre lavorare per superare egoismi e diffidenze.

Ricorda che, rispetto al Quadro congiunto per contrastare le minacce ibride, che propone un approccio esteso a tutti i livelli dell'amministrazione per rafforzare la resilienza globale delle società e individua 22 azioni concrete, la Relazione in esame ha lo scopo di riferire in merito ai progressi compiuti e alle prossime fasi di attuazione rispetto alle azioni nelle quattro aree prioritarie proposte dal Quadro congiunto.

Passando ad illustrare le singole azioni previste dal Quadro congiunto e il loro stato di attuazione in base alla Relazione, segnala che in merito all'Azione 1, che invita gli Stati membri a procedere a uno studio sui rischi ibridi per individuare le vulnerabilità principali delle strutture e reti nazionali e paneuropee, il Consiglio ha istituito un Gruppo degli amici della presidenza, gruppo informale con funzioni preparatorie del COREPER, al fine di creare uno strumento di indagine generale che 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. Segnala che nella Relazione si prevede che lo strumento di indagine dovrebbe essere pronto entro la fine dell'anno, in vista dell'inizio delle indagini che gli Stati membri sono invitati a realizzare. Evidenzia che sul lavoro svolto dal Gruppo sarebbe auspicabile che il Governo italiano, che vi partecipa con i propri rappresentanti, fornisse informazioni più puntuali rispetto a quelle scarne già disponibili e una sua valutazione sulla relativa utilità. Ritiene che sul punto e più complessivamente sul provvedimento sarebbe auspicabile invitare in audizione il

Rappresentante Permanente d'Italia presso l'Unione europea, Ambasciatore Maurizio Massari.

Segnalando che l'Azione 2 prevede la creazione di una cellula dell'UE per l'analisi delle minacce ibride, ricorda che tale cellula è stata costituita alla fine del 2016 presso il centro di analisi dell'*intelligence* dell'Unione e le sue analisi sono condivise nell'UE e negli Stati membri (gli Stati membri sono invitati a istituire punti di contatto nazionali). Sottolinea che da gennaio 2017 la cellula realizza un bollettino di informazione periodico sulle minacce ibride che analizza. Inoltre, segnala che la cellula esamina le iniziative per potenziare la cooperazione UE-NATO. A tale proposito ritiene opportuno capire se i bollettini di informazioni predisposti dalla stessa cellula si siano rivelati utili e quale seguito venga dato loro.

In merito all'Azione 3, riguardante l'aggiornamento e coordinamento delle capacità per la formulazione di comunicazioni strategiche proattive, segnala che l'Alta Rappresentante Mogherini ha istituito la *task force* East StratCom, la quale ha il compito di formulare previsioni e reagire alle campagne e ai casi di disinformazione della Federazione russa, migliorando la comunicazione relativa alle politiche dell'Unione nei Paesi del vicinato orientale. Al riguardo fa presente di avere visitato a Riga l'equivalente centro della NATO e di avere maturato una nuova consapevolezza circa la notevole qualità e quantità di dati raccolti sull'attivismo di provenienza russa. Nell'ambito dell'Azione 3, segnala, altresì, il nuovo sito *web www.euvsdisinfo.eu*, che permette di cercare online le attività di disinformazione, e il progetto EU-STRAT, che è finanziato dal programma di ricerca e sviluppo dell'UE Orizzonte 2020 e che analizza la politica e i *media* nei Paesi del partenariato orientale. Infine, ricorda che la Commissione europea finanzia anche la Rete europea per la comunicazione strategica, che ha lo scopo di condividere analisi, buone pratiche e idee sull'uso delle comunicazioni strategiche nella lotta contro l'estremismo violento e la disinformazione. A tale proposito, comunica di aver visitato lo *Strategic Communications Centre of Excellence* della NATO, che reputa particolarmente all'avanguardia.

Riguardo all'Azione 4, volta all'istituzione di un centro di eccellenza per la lotta contro le minacce ibride, ricorda che, nell'aprile 2017, la Finlandia – ritenuto un Paese particolarmente avanzato per gli studi in questo settore – ha creato il centro europeo per la lotta contro le minacce ibride, di cui sono componenti 10 Stati membri dell'UE (Finlandia, Francia, Germania, Lettonia, Lituania, Polonia, Regno Unito, Estonia e Spagna), la Norvegia e gli Stati Uniti. Segnala che il centro promuove il dialogo strategico e la realizzazione di attività di ricerca e analisi al fine di migliorare la resilienza e la capacità di risposta alle minacce ibride. Sottolinea che attività del centro sono complementari a quelle svolte dalla cellula per l'analisi delle minacce ibride dell'UE, con cui opera in stretto contatto. Ritiene opportuno che il Governo chiarisse le ragioni per cui fino ad ora il nostro Paese non ha preso parte al centro europeo contro le minacce ibride.

Ricorda che l'Azione 5 prevede l'individuazione di strumenti comuni, compresi indicatori, per migliorare la protezione e la resilienza delle infrastrutture critiche a fronte delle minacce ibride. In tale ambito, segnala che nel 2017, nel corso di un seminario sulle minacce ibride organizzato dalla Commissione europea, sono state concordate una tabella di marcia comune e azioni da intraprendere per il futuro. A tale proposito, evidenzia che la Commissione consulterà nuovamente le parti interessate con l'obiettivo di giungere a un accordo sull'individuazione degli indicatori entro la fine del 2017. Inoltre, sottolinea che, entro la fine dell'anno, l'Agenzia europea per la difesa dovrebbe presentare 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.

In merito all'Azione 6, che prevede la diversificazione delle fonti di energia e la

promozione di norme di sicurezza e protezione per le infrastrutture nucleari, ricorda i progressi compiuti in ambito UE nello sviluppo di progetti chiave per diversificare rotte e fonti energetiche (ad esempio, il corridoio meridionale di trasporto del gas) e la proposta di regolamento sulla sicurezza dell'approvvigionamento di gas, attualmente all'esame delle istituzioni europee. Inoltre, pone l'accento sulla necessità di migliorare l'utilizzo delle fonti energetiche autoctone, in particolare quelle rinnovabili. Quanto alla sicurezza nucleare, ricorda che gli Stati membri sono chiamati a dare attuazione a due direttive sulla sicurezza nucleare e sulle norme fondamentali di sicurezza entro la fine, rispettivamente, del 2017 e del 2018.

Segnala che l'Azione 7 prevede il monitoraggio delle minacce emergenti nel settore dei trasporti. A tale proposito, ricorda che la Commissione europea ha elaborato una metodologia di valutazione del rischio comune della UE nell'ambito della sicurezza aerea, che consente lo scambio di informazioni riservate e la definizione di un quadro del rischio comune. Sottolinea che, nel corso del 2018, la Commissione intende formulare proposte per espandere tale valutazione anche ad altre modalità di trasporto, posta la evidente asimmetria che allo stato si determina tra i livelli dei controlli e delle misure di prevenzione applicati, rispettivamente, al controllo aereo e al controllo ferroviario. A tale proposito, segnala come emerga una questione relativa al bilanciamento di due interessi contrapposti: quello della garanzia della sicurezza e quello della tutela della *privacy,* e come tale bilanciamento risponda a diverse sensibilità nel raffronto tra l'Europa e gli Stati Uniti. Inoltre, segnala che la Commissione, in collaborazione con l'Agenzia europea per la sicurezza aerea, sta sviluppando due iniziative per rafforzare la cibersicurezza, volte all'istituzione di una squadra di pronto intervento informatico in materia di aviazione e alla 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). Relativamente alle dogane, segnala che, al fine di identificare in modo più efficace e tempestivo le spedizioni ad alto rischio, la Commissione intende potenziare il sistema di informazioni anticipate sui carichi e di gestione dei rischi doganali.

In merito all'Azione 8, volta a incrementare la resilienza delle infrastrutture spaziali contro le minacce ibride, segnala che la Commissione ha intenzione di integrare questo aspetto nella predisposizione del quadro normativo relativo alla comunicazione satellitare governativa (GovSatCom) e alla sorveglianza dello spazio e al tracciamento. Inoltre, sottolinea che, nel predisporre 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.

Ricorda che l'Azione 9 prevede la definizione di progetti relativi alle possibilità di adattamento delle capacità di difesa degli Stati membri specificamente contro le minacce ibride. A tale proposito, segnala che la Relazione indica che le priorità in termini di capacità individuate dagli Stati membri ai fini del rafforzamento della resilienza contro le minacce ibride potrebbero essere ammissibili al sostegno nell'ambito del Fondo europeo per la difesa già a partire dal 2019.

Ricorda che l'Azione 10 ha lo scopo di aumentare la conoscenza delle minacce ibride e la resilienza nell'ambito dei meccanismi di preparazione e coordinamento esistenti, come il comitato per la sicurezza sanitaria contro gli attacchi di natura batteriologica. Da questo punto di vista, segnala che la Commissione sostiene gli Stati membri tramite formazione ed esercizi di simulazione, anche favorendo lo scambio di linee guida basate sull'esperienza e finanziando azioni comuni. A tale proposito, sottolinea che la Commissione e gli Stati membri stanno preparando un'azione comune per prevenire e fronteggiare la diffusione transfrontaliera di malattie,

operando anche al fine di rafforzare l'offerta di vaccini e migliorare la sicurezza sanitaria a livello dell'UE.

Riguardo all'Azione 11, che prescrive il pieno utilizzo della rete fra i 28 *Computer Security and Incident Response Team* (CSIRT) nazionali e la squadra di pronto intervento informatico dell'Unione (CERT-UE), segnala che è stata adottata la direttiva (UE) 2016/1148 sulla sicurezza delle reti e i sistemi informativi, che ha introdotto le prime norme in materia di cibersicurezza, rafforzando la collaborazione tra gli Stati membri. Sottolinea che tale direttiva ha istituito la rete di gruppi di intervento per la sicurezza informatica in caso di incidente; specifica che, parallelamente, la Commissione e la CERT-UE procedono a un attivo monitoraggio delle minacce informatiche e allo scambio di informazioni con le autorità nazionali, al fine di garantire che i sistemi informatici delle istituzioni europee siano sicuri e resilienti agli attacchi informatici. Ricorda che i recenti attacchi informatici a livello mondiale hanno disattivato migliaia di sistemi informatici evidenziando l'urgente necessità di rafforzare la resilienza informatica e le azioni di sicurezza all'interno della UE. Evidenzia che nel maggio 2017 l'incidente causato dal *ransomware* WannaCry ha rappresentato la prima occasione per la rete europea di scambio operativo di informazioni e di cooperazione grazie alla diffusione di raccomandazioni. Segnala che lo scambio di relazioni nazionali sulla situazione ha prodotto una consapevolezza situazionale comune in tutta l'Unione e tale esperienza ha permesso alla rete di essere meglio preparata ai successivi incidenti.

Ricorda che l'Azione 12 prevede la collaborazione con l'industria nel contesto di un partenariato pubblico-privato sulla cibersicurezza, al fine di sviluppare tecnologie volte a proteggere maggiormente gli utenti e le infrastrutture dagli aspetti informatici delle minacce ibride. A tale proposito, segnala che nel 2016 la Commissione, in coordinamento con gli Stati membri, ha firmato con l'industria un partenariato pubblico-privato sulla cibersicurezza, il quale 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 ed ibride. A tale proposito ritiene particolarmente importante procedere celermente alla ratifica della Convenzione di Budapest.

Nell'ambito dell'Azione 13, volta alla definizione di orientamenti destinati ai detentori di risorse della rete intelligente per migliorare la cibersicurezza dei loro impianti, segnala che nel settore dell'energia la Commissione sta preparando una strategia settoriale sulla cibersicurezza, che prevede l'istituzione di una piattaforma per la cibersicurezza degli esperti di energia con lo scopo di rafforzare l'attuazione della direttiva (UE) 2016/1148. Ricorda che l'attuazione di tale direttiva è prevista nella legge di delegazione europea 2016-2017, attualmente in corso di esame presso la Camera (C. 4620). Inoltre, segnala che, in attesa dell'attuazione di tale direttiva, in Italia, con il DPCM del 17 febbraio 2017, sono stati previsti la redazione di un piano nazionale per la protezione cibernetica e la sicurezza informatica e il rafforzamento del ruolo del Comitato interministeriale per la sicurezza della Repubblica (CISR), il quale avrà il compito di emanare direttive con l'obiettivo di innalzare il livello della sicurezza informatica del Paese.

Ricorda che l'Azione 14 ha lo scopo di promuovere piattaforme e reti di scambio di informazioni sulle minacce ibride nel settore finanziario. A tale proposito, segnala che, al fine di migliorare la sicurezza degli strumenti di pagamento, in particolare *online*, è stata approvata la direttiva (UE) n. 2015/2366. Inoltre, sottolinea che la Commissione, in collaborazione con l'Autorità bancaria europea e le parti interessate, sta elaborando norme tecniche di regolamentazione in materia di autenticazione del cliente. Evidenzia che la Commissione ha, altresì, annunciato la presentazione di 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, incluse quelle tramite valute virtuali.

Segnala che l'Azione 15, che prevede la promozione della lotta alle minacce ibride relative agli attacchi informatici nel settore dei trasporti, dovrebbe esplicitarsi sostanzialmente nell'attuazione del piano di azione relativo alla strategia per la sicurezza marittima della UE. Inoltre, ricorda che, entro il 2017, dovrebbe essere completato un programma congiunto, civile e militare, della Commissione e del SEAE in materia di ricerca strategica nel settore della sicurezza, con un *workshop* finale sulla protezione delle infrastrutture marittime critiche. Sottolinea che tali lavori, in futuro, potrebbero essere ampliati allo scopo di esaminare le minacce emergenti connesse a interferenze oltre il confine delle acque nazionali e riguardanti condotte sottomarine, il trasferimento di energia e il cablaggio per la comunicazione tradizionale e in fibra ottica.

Ricorda che l'Azione 16 prevede che la Commissione sfrutti l'attuazione del piano di azione contro il finanziamento del terrorismo anche per contribuire alla lotta contro le minacce ibride. Segnala che, in quest'ottica, nel dicembre 2016, la Commissione ha presentato tre proposte legislative che riguardavano, tra l'altro, sanzioni penali in materia di riciclaggio di denaro, di controlli sul denaro contante in entrata e in uscita dall'Unione e di congelamento e confisca di beni. Segnala, poi, che l'Italia, con il decreto legislativo n. 90 del 2017, ha recepito la direttiva antiriciclaggio, che rafforza l'obbligo di valutazione del rischio per banche, avvocati e contabili; prevede chiari requisiti di trasparenza per le imprese circa la titolarità effettiva; semplifica la cooperazione e lo scambio di informazioni; rafforza i poteri sanzionatori. Infine, segnala che, nel luglio 2016, la Commissione ha adottato una proposta, attualmente all'esame del Parlamento europeo e del Consiglio dell'UE, che ha lo scopo di rafforzare ulteriormente la normativa antiriciclaggio.

In merito all'Azione 17, che ha lo scopo di rafforzare le procedure di eliminazione dei contenuti illegali da Internet, ricorda che la Commissione sta portando avanti l'attuazione della strategia di risposta alla radicalizzazione, contenuta nella comunicazione « Sostenere la prevenzione della radicalizzazione che porta all'estremismo violento ». Sottolinea che tale strategia definisce 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 collaborazione con Paesi terzi. Inoltre, ricorda che, tramite l'unità UE addetta alle segnalazioni su Internet di Europol e il Forum dell'UE su Internet, la Commissione ha adottato provvedimenti per ridurre la disponibilità di contenuti illegali *online*. Infine, evidenzia che, nell'ambito della strategia per il mercato unico digitale, la Commissione vuole garantire un migliore coordinamento del dialogo con le piattaforme *online*, incentrandolo sui meccanismi e sulle soluzioni tecniche in materia di rimozione dei contenuti illegali.

Coglie questa opportunità per segnalare l'*iter* di esame, in corso al Senato, del disegno di legge, già licenziato dalla Camera, di ratifica ed esecuzione del Protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica, riguardante la criminalizzazione degli atti di razzismo e xenofobia commessi a mezzo di sistemi informatici, fatto a Strasburgo il 28 gennaio 2003.

A tale proposito, ricorda l'impegno del Parlamento italiano sul terreno della deradicalizzazione, cui si sono dedicati in particolare i colleghi Manciulli e Dambruoso con la proposta di legge che ha inteso introdurre in Italia una strategia per la prevenzione dei fenomeni di radicalizzazione e di diffusione dell'estremismo jihadista, nonché provvedere al recupero umano, sociale, culturale e professionale di soggetti già coinvolti in fenomeni di radicalizzazione, mediante programmi di formazione ed informazione

che interessino la società civile e le istituzioni a tutti i livelli, comprese le istituzioni scolastiche e le carceri.

Ricorda che l'Azione 18 prevede l'avvio di uno studio sui rischi ibridi nelle regioni del Vicinato. A tale proposito, segnala che l'Unione europea si è concentrata sul rafforzamento delle capacità e della resilienza nei Paesi partner nel settore della sicurezza, sottolineando la connessione tra sviluppo e sicurezza e avviando dialoghi sulla sicurezza e sul contrasto al terrorismo con i Paesi del Mediterraneo. Inoltre, segnala che è stato avviato un progetto pilota per lo studio dei rischi in collaborazione con la Repubblica di Moldova, con l'obiettivo di individuare le principali vulnerabilità del Paese e canalizzare in quei settori l'assistenza da parte della UE. Sottolinea che, basandosi sull'esperienza acquisita, la Commissione e il SEAE raccomanderanno di dare priorità alle azioni relative alla promozione dell'efficacia, della comunicazione strategica, della protezione delle infrastrutture critiche e della cibersicurezza. Infine, segnala che, a luglio 2017, la Commissione e l'Alta Rappresentante Mogherini hanno adottato una comunicazione congiunta su « Un approccio strategico alla resilienza nell'azione esterna dell'UE », che rappresenta la necessità di abbandonare gli obiettivi di contenimento delle crisi per orientarsi verso un approccio alle vulnerabilità più strutturale e di lungo termine.

In merito all'Azione 19, che prevede la definizione di un protocollo operativo comune ed esercizi regolari per migliorare la capacità decisionale strategica in risposta alle minacce ibride, segnala che la Commissione e l'Alta Rappresentante hanno presentato un protocollo (EU-Playbook) che individua le modalità operative che l'Unione intende attivare in caso di minacce ibride, allo scopo di garantire un migliore coordinamento delle azioni di contrasto a tali minacce tra i vari livelli decisionali, operativi e tecnici e i partner esterni, in particolare la NATO. Sottolinea che, analogamente, la NATO ha elaborato un manuale tattico per una maggiore interazione NATO-UE per la prevenzione e il contrasto delle minacce ibride in materia di ciberdifesa, comunicazione strategica, consapevolezza situazionale e gestione delle crisi.

Ricorda che l'Azione 20 prevede la verifica dell'applicabilità e delle implicazioni pratiche dell'articolo 222 del TFUE (clausola di solidarietà) e dell'articolo 42, paragrafo 7, del TUE (obbligo di prestare aiuto e assistenza in caso di aggressione armata ad altro Stato membro dell'UE) in caso di attacchi ibridi gravi e di vasta portata. Segnala che nella Relazione si specifica che, in caso di attacchi ibridi, che sono una combinazione di azioni criminali e sovversive, è più probabile il ricorso all'articolo 222 del TFUE, secondo le modalità di attuazione previste dalla decisione 2014/415/UE del Consiglio. Tuttavia, sottolinea che, se un attacco ibrido si svolgesse anche tramite un'azione armata, potrebbe essere invocato l'articolo 42, paragrafo 7, del TUE. Evidenzia che, in questo caso, l'aiuto e l'assistenza sarebbero forniti sia dagli Stati membri sia dall'Unione.

Riguardo all'Azione 21, che prevede il coordinamento da parte dell'Alta Rappresentante delle capacità di azione militare nella lotta contro le minacce ibride nell'ambito della politica di sicurezza e difesa comune, segnala che il Comitato militare dell'UE ha presentato il parere sul contributo militare dell'Unione alla lotta contro le minacce ibride nell'ambito della PSDC e che in tale parere si sottolinea la necessità di una maggiore cooperazione tra i servizi di *intelligence* militare e la cellula dell'UE per l'analisi delle minacce ibride.

Infine, ricorda che l'Azione 22 prevede il rafforzamento della cooperazione e del coordinamento con la NATO. Sottolinea che, in base alla dichiarazione congiunta siglata l'8 luglio 2016 a Varsavia dai presidenti del Consiglio europeo e della Commissione europea e dal segretario generale della NATO, l'Unione europea e la NATO hanno sviluppato un insieme comune di 42 proposte di attuazione della cooperazione. Segnala che la lotta alle minacce ibride è uno dei sette settori di cooperazione in-

dividuati nella dichiarazione congiunta e riguarda ben 10 delle 42 proposte di attuazione. Evidenzia che, per la prima volta, il personale della NATO e quello dell'UE effettueranno esercitazioni congiunte per rispondere a uno scenario ibrido.

Concludendo, sottolinea che dalla Relazione in esame emerge che la Commissione e l'Alta Rappresentante Mogherini hanno raggiunto risultati in tutti gli ambiti previsti dal Quadro congiunto, in stretta cooperazione con gli Stati membri e i partner. Tuttavia, ritiene importante non perdere lo slancio di fronte alle minacce ibride attuali, che sono in costante evoluzione. Sottolinea che la Relazione esorta gli Stati membri a procedere sulla strada del contrasto alle minacce ibride, in quanto ad essi spetta la responsabilità principale della lotta alle minacce attinenti alla sicurezza nazionale e al mantenimento dell'ordine pubblico. A tale proposito, segnala che la forza dell'intervento dell'Unione europea consiste nell'assistere gli Stati membri e i partner nel rafforzamento della loro resilienza sulla base di una vasta gamma di programmi e strumenti esistenti. Evidenzia che per questo motivo la Commissione e l'Alta Rappresentante invitano gli Stati membri e le parti interessate, quando sia necessario, a raggiungere rapidamente un accordo e a garantire una rapida ed efficace azione delle diverse misure volte a rafforzare la resilienza delineate nella Relazione in esame.

In conclusione, crede che il documento in esame rivesta un indiscutibile rilievo per due ordini di motivi: in primo luogo, perché fornisce un quadro dettagliato e puntuale sui progressi realizzati e, contestualmente, sulle cose che ancora occorre fare per tradurre su un piano concreto l'impegno a prevenire e contrastare le minacce ibride. In secondo luogo, ritiene che, attraverso la Relazione, i Parlamenti hanno la possibilità di svolgere un attento controllo sulla idoneità e sull'efficacia delle iniziative adottate e possono sollecitare i rispettivi governi a riferire sul contributo fornito e sui progressi che possono e devono essere realizzati a livello nazionale e a livello europeo.

Andrea MANCIULLI, *presidente,* nessun altro chiedendo di intervenire, rinvia il seguito del dibattito ad altra seduta.

La seduta termina alle 13.55.

UFFICIO DI PRESIDENZA INTEGRATO DAI RAPPRESENTANTI DEI GRUPPI

L'ufficio di presidenza si è riunito dalle 13.55 alle 14.