CAMERA DEI DEPUTATI

Doc. **XVIII** N. **96**

COMMISSIONI RIUNITE I (AFFARI COSTITUZIONALI, DELLA PRESIDENZA DEL CONSIGLIO E INTERNI) E III (AFFARI ESTERI E COMUNITARI)

DOCUMENTO FINALE, A NORMA DELL'ARTICOLO 127 DEL REGOLAMENTO SU:

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)

Approvato l'8 novembre 2017

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

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)

DOCUMENTO FINALE APPROVATO

Le Commissioni riunite I (Affari costituzionali, della Presidenza del Consiglio e interni) e III (Affari esteri e comunitari);

esaminata, ai sensi dell'articolo 127 del Regolamento, la relazione sull'attuazione del Quadro congiunto per contrastare le minacce ibride (JOIN(2017)30) presentata congiuntamente dalla Commissione europea e dall'Alta Rappresentante per gli affari esteri e la politica di sicurezza;

rilevato che:

la relazione illustra i progressi realizzati nell'ambito di tale Quadro congiunto e gli obiettivi delle ulteriori misure che intendono presentare per contrastare le cosiddette « minacce ibride »;

nelle valutazioni della Commissione europea, si intendono per minacce ibride le attività, che quasi sempre combinano metodi convenzionali e non convenzionali che possono essere realizzate in modo coordinato da soggetti diversi dalle entità statuali, il cui 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;

si tratta 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 derivare;

la natura transnazionale di tali minacce impone la necessità di adottare strategie di prevenzione e contrasto comuni, in primo luogo a livello europeo, volte a coordinare e supportare l'azione degli Stati membri ai quali compete la responsabilità principale nel contrasto alle minacce ibride;

è quindi indispensabile un approccio integrato che deve tenere conto sia della dimensione della politica estera dell'UE sia delle politiche interne dell'UE;

si tratta, dunque, di porre in essere una serie di iniziative coerenti dirette a realizzare una migliore capacità di intercettare con ampio anticipo e monitorare le minacce; di rafforzare la resilienza (in particolare per quanto riguarda i trasporti, le comunicazioni, l'energia, i sistemi finanziari e le infrastrutture di sicurezza); di promuovere la capacità degli Stati membri e dell'Unione di agire in modo coordinato; di rafforzare la cooperazione con la NATO;

nell'auspicio che:

con riferimento all'Azione 1, il Governo possa fornire, nelle opportune sedi parlamentari, elementi sull'attività svolta nell'ambito del Gruppo di lavoro istituito dal Consiglio con funzioni preparatorie del COREPER, incaricato di individuare entro la fine dell'anno i principali indicatori delle minacce ibride, ad integrarli nei meccanismi di allarme rapido, di valutazione e di condivisione dei rischi esistenti;

con riferimento all'Azione 2, concernente l'istituzione di una cellula dell'UE per l'analisi delle minacce ibride, nell'intento di potenziare la cooperazione tra l'UE e la NATO, possa essere altresì segnalata, in sede parlamentare, la portata dei bollettini di informazione predisposti dalla stessa cellula e la necessità di una maggiore cooperazione tra i servizi di *intelligence* militare e la cellula dell'UE per l'analisi delle minacce ibride;

con riferimento all'Azione 4, l'Italia voglia siglare il *memorandum of understanding* per la creazione di un *European Centre of Excellence for Countering Hybrid Threats* siglato ad Helsinki il 12 aprile 2017, con cui è stato istituito in Finlandia il Centro europeo per la lotta contro le minacce ibride;

con riferimento all'Azione 16, richiamato il decreto legislativo n. 90 del 25 maggio 2017 di recepimento della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006;

evidenziato, con riferimento all'Azione 17, l'impegno profuso dal Parlamento italiano sul terreno della deradicalizzazione nella prospettiva della approvazione anche da parte del Senato del provvedimento recante « Misure per la prevenzione della radicalizzazione e dell'estremismo violento di matrice jihadista », già licenziato dalla Camera dei deputati;

raccolto in generale l'appello della Commissione e dell'Alta Rappresentante per il rapido raggiungimento di accordi tra gli Stati membri nell'interesse del rafforzamento della resilienza europea contro le minacce ibride;

rilevata la necessità che il presente documento finale sia trasmesso tempestivamente alla Commissione europea, nell'ambito del cosiddetto dialogo politico, nonché al Parlamento europeo e al Consiglio;

esprimono

UNA VALUTAZIONE FAVOREVOLE

con le seguenti osservazioni:

a) ai fini di una più efficace attività di prevenzione e contrasto delle diverse tipologie di minacce ibride, appare indispensabile realizzare una collaborazione più stretta, anche sperimentando forme originali di partenariato, con i Paesi terzi e, in particolare, con quelli che si trovino nelle aree più direttamente investite da fenomeni terroristici o da conflitti e instabilità, in modo da responsabilizzarli e allo stesso tempo da consolidarne la capacità di reazione;

b) carattere prioritario, ai fini della prevenzione e del monitoraggio delle minacce, assume la realizzazione, attraverso l'adozione di tutti gli strumenti informatici utili, e con le opportune cautele a salvaguardia della riservatezza dei dati, un costante ed efficace scambio di informazioni fra le strutture specializzate degli Stati membri, le agenzie dell'Unione europea più direttamente investite nella materia e i corrispondenti organismi degli Stati terzi maggiormente coinvolti;

c) tra le azioni da realizzare, carattere assolutamente prioritario assume il rafforzamento degli strumenti di protezione e resilienza delle cosiddette infrastrutture critiche. A tal fine, si raccomanda la massima attenzione nella definizione degli indicatori di vulnerabilità e nella evidenziazione delle lacune e delle carenze cui occorre porre rimedio con urgenza;

d) fra le infrastrutture critiche, particolare attenzione dovrà essere dedicata al comparto dei trasporti, stante l'evidente asimmetria che attualmente si registra per quanto concerne il livello dei controlli e della sicurezza tra il settore aereo e le

altre modalità di trasporto, in particolare quelli ferroviario e marittimo. A quest'ultimo proposito, è auspicabile un rafforzamento delle misure di prevenzione relativamente alla circolazione dei mezzi navali di maggiori dimensioni, sia per il trasporto passeggeri sia per il traffico commerciale, specie per quanto concerne il trasporto di fonti energetiche e di merci pericolose, particolarmente esposti ad attacchi e minacce ibride;

e) massima attenzione dovrà essere assicurata anche alla protezione dei siti che ospitano centrali nucleari in considerazione dell'ampiezza delle aree geografiche che potrebbero essere investite dalle conseguenze di un attacco, che supererebbe i confini degli Stati membri che ospitano le centrali stesse;

f) occorre, inoltre, limitare quanto più possibile i rischi che possono discendere da attacchi mossi alle infrastrutture informatiche e ai sistemi di rete, suscettibili di paralizzare l'attività di interi Paesi o di settori molto ampi, stante il fatto che già si registrano sempre più frequenti e invasivi attacchi informatici e alle reti di comunicazione.

17018002298O