LA PROTEZIONE DEL TRASPORTO AEREO NELL'UE DALLE MINACCE "HYBRID" E "CYBER"

di DORIANO RICCIUTELLI
Consulente ENAC

La Commissione il 13 giugno 2018 ha inoltrato la comunicazione[1] congiunta al Parlamento, al Consiglio europeo e al Consiglio sull'attuazione del Quadro congiunto per contrastare le minacce ibride contenente complessivamente una serie di 22 azioni volte a migliorare la capacità di rilevare con tempestività le aggressioni di tale natura e consolidare la resilienza delle istituzioni e delle infrastrutture critiche della società quali, inter alia, il trasporto aereo.

Quanto alla genesi dell'iniziativa in parola occorre preliminarmente risalire alla comunicazione originaria del 6 aprile 2016 (Join (2016) 18 final) promossa dall'Alto rappresentante, in stretta cooperazione con i servizi della Commissione e con l'Agenzia europea per la Difesa (AED) resasi necessaria all'Unione per fortificarsi quale garante della sicurezza, alla luce delle grandi sfide alla pace e alla stabilità degli Stati membri.

Nel panorama dei progressi conseguiti durante quest'ultimo anno – rispetto a quanto riscontrato nella prima, analoga relazione del 2017 – rileva il chiaro rafforzamento delle potenzialità dei paesi europei di prevenire le crisi, produrre idonee reazioni e riprendersi in modo rapido e coordinato, nonché la fattiva cooperazione con la NATO per assicurare la complementarità delle misure ed il riconoscimento della natura ibrida delle minacce (i.e. attacchi elettronici ai sistemi aeroportuali e di controllo dei voli).

In proposito, pur assumendo che le definizioni dell'accezione "minacce ibride" variano e devono conservare un pur minimo livello di flessibilità "per rispondere al loro carattere mutevole", il relativo concetto portante, invece, è orientato ad esprimere la "combinazione di attività coercitive e sovversive, di metodi convenzionali e non convenzionali (cioè diplomatici, militari, economici e tecnologici), utilizzabili in maniera coordinata da entità statali o non per raggiungere determinati obiettivi di destabilizzazione, comunque sempre "*rimanendo al di sotto della soglia di una guerra ufficialmente dichiarata*".

Sul terreno dei temi dominanti l'interesse degli organi comunitari è incentrato (azione 7) sulla circostanza che gli attacchi ibridi alle infrastrutture come gli aeroporti e gli impianti dedicati al controllo aereo possono determinare gravi conseguenze e perturbare il trasporto oltre alle catene di approvvigionamento e, in tale contesto, forma oggetto di approfondito dibattito proprio la rivisitazione della sicurezza aerea, che rientra nell'alveo della strategia per l'aviazione in Europa.
In particolare la Commissione, in coordinamento con gli Stati membri, è impegnata (nel quadro dell'azione 11) ad analizzare le minacce informatiche – un vero *leitmotiv* dell'intera iniziativa – e i corrispondenti rischi legati alle interferenze illecite con i sistemi del trasporto aereo, elaborando una tabella di marcia per una sicurezza specifica nell'aviazione in cooperazione con l'Agenzia europea per la sicurezza aerea (EASA).

Ancorché si sia in grado di vantare notevoli progressi sul fronte della cyber sicurezza, non può, invero, escludersi per contro l'esistenza di elementi di vulnerabilità dei sistemi (i.e. un guasto tecnico o una minaccia informatica), come verificatisi dal recente incidente occorso ad Eurocontrol, che ha riguardato un considerevole numero dei voli in Europa.

La Commissione europea, congiuntamente all'Agenzia EASA, ha già istituito la squadra di pronto intervento informatico in materia di aviazione e creato una task force per la cyber sicurezza nel *framework* dell'impresa comune per la ricerca sulla gestione del traffico aereo nel cielo unico europeo (SESAR).

In questa ottica muove la nuova legislazione europea sulla citata riforma dell'Agenzia (regolamento 1139/18 del 4 luglio 2018), contenente giustappunto le misure di regolamentazione dell'aviazione civile e gli atti delegati nonché di esecuzione della Commissione, che dovranno "*corrispondere ed essere proporzionati alla natura e ai rischi dei diversi tipi di aeromobili, operazioni e attività che disciplinano*". A nostro avviso, in sede unionale si è convenientemente introdotto un disegno normativo che risponde appieno alla esigenza di fronteggiare, a seguito di una valutazione dei rischi, le eventuali carenze nella progettazione degli aeromobili ovvero di raccomandare le misure correttive

LA PROTEZIONE DEL TRASPORTO AEREO NELL'UE DALLE MINACCE "HYBRID" E "CYBER" *segue*

adottabili da parte delle autorità nazionali competenti o delle persone fisiche e giuridiche operanti nel comparto aereo, nel caso di problematiche insorgenti correlate all'esercizio degli aeromobili.

Appare corretto sostenere che tali misure, per quanto possibile, promuoveranno, altresì, un proficuo approccio sistemico all'aviazione civile, tenendo conto delle interdipendenze tra sicurezza e altri ambiti della normativa aeronautica tra cui, *in primis,* la cyber sicurezza, per ottenere più efficientemente i livelli di security prescritti in termini di costi e stimolare l'innovazione tecnica e operativa.

A tal fine e, segnatamente, per contribuire più incisivamente alla protezione dell'aviazione civile da atti di interferenza illecita nel caso di accertamento delle predette interdipendenze tra safety, security e cyber sicurezza, l'Agenzia, se necessario, reagisce immediatamente ai problemi urgenti di mutuo interesse per gli Stati membri.

Infatti, allorché si verifichi la coesistenza di correlazioni tra safety e security nell'aviazione civile, l'Agenzia, sulla base delle proprie pertinenti competenze in materia, presta, su richiesta, assistenza tecnica alla Commissione per l'attuazione del regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio e di altre disposizioni afferenti al diritto dell'Unione.

Restando a riflettere di cyber sicurezza, non sembra fuori luogo soggiungere che recentemente gli Stati membri hanno emanato norme vincolanti per recepire la direttiva sulla sicurezza delle reti e dei sistemi d'informazione (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 (Direttiva NIS – Network and information Security).

In Italia si è provveduto attraverso il decreto legislativo di attuazione del 18 maggio 2018, n. 65 che stabilisce puntuali misure volte a conseguire un livello elevato di sicurezza della rete e dei sistemi informativi a livello nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea.

Riguardo al contesto aereo di cui qui si argomenta, il suddetto provvedimento designa quali Autorità competenti NIS il Ministero delle infrastrutture e dei trasporti per il settore trasporti, sottosettore aereo e indica, quali operatori dei servizi essenziali, i vettori aerei definiti dal regolamento (CE) n. 300/2008 (cit.) riguardante la security dell'aviazione civile, i gestori aeroportuali, aeroporti e controllori del traffico aereo.

Gioca un ruolo fondamentale in questa fase la prossima adozione del Cybersecurity Act (proposta di regolamento del 22.2.2018 COM (2017) 477 final/3) che, in perfetto *pendant* con la direttiva NIS, potrà opportunamente rappresentare una parte della nuova strategia dell'Unione, rivolta a *"rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali".*

In tale prospettiva l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) avrebbe il compito di partecipare attivamente alla formulazione della politica in materia di sicurezza delle reti e dell'informazione, nonché allo sviluppo di altre iniziative che presentano elementi di cyber sicurezza in diversi rami trasporti nonché, tra l'altro, la consulenza e il coordinamento settoriale in siffatta materia nel trasporto aereo .

In parallelo si noti che - quale tangibile apporto alla riunione dei leader del 19-20 settembre 2018 a Salisburgo - la Commissione europea ha avviato l'esame legislativo di una proposta di regolamento (COM (2018) 630 final) istitutiva di un Centro europeo di competenze in materia di cyber sicurezza con il compito di gestire un mirato sostegno finanziario proveniente dal bilancio dell'UE e di facilitare gli investimenti congiunti da parte dell'Unione, degli Stati membri e dell'industria per promuovere tale settore garantendo che i sistemi di difesa risultino all'avanguardia .

Ma v'è di più. Nel mentre, difatti, prosegue l'impegno a fronteggiare il tema della cybersecurity in seno al comitato AVSEC della Commissione (ex art. 19 regolamento UE 300/08, cit.), per un verso, tramite gli incontri (il più recente risalente all'11 dicembre 2018) con il gruppo SAGAS rappresentativo dell'industria aeroportuale e, per altro verso, con la preparazione del testo per il recepimento dello standard ICAO 4.9.1 (in vigore dal 26 novembre 2018) che verrà sottoposto al vaglio

LA PROTEZIONE DEL TRASPORTO AEREO NELL'UE DALLE MINACCE "HYBRID" E "CYBER"

dei componenti del citato comitato il 19 marzo 2019 [2].

In particolare si tratta della regola secondo la quale ciascuno Stato contraente, in conformità alla valutazione dei rischi effettuata dalle proprie designate competenti autorità nazionali, dovrebbe garantire che siano elaborate misure appropriate per difendere la riservatezza, l'integrità e la disponibilità dei sistemi critici di informazione e della tecnologia delle comunicazioni e dei dati utilizzati per l'aviazione civile da interferenze che possano mettere a repentaglio la security aerea ed aeroportuale.

Al di là delle questioni di cyber sicurezza e, conformemente alle raccomandazioni, la Commissione ha inoltre elaborato, con il sostegno di esperti nazionali nel campo dell'aviazione e del SEAE (Servizio Europeo per l'azione esterna), 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.

Non va sottaciuto che sul versante della problematica aperta sulla sicurezza cibernetica il 18 ottobre 2018 (EUCO 13/18), il Consiglio europeo ha chiesto di supportare - portando a termine i negoziati su tutte le proposte in materia – ulteriori misure per combattere le minacce di tipo cyber per contrastare le attività illecite e dolose di siffatta natura, basate sull'uso di sistemi informatici e quindi creare una solida struttura di cyber sicurezza.

Nel prosieguo della nostra disamina non omettiamo di cogliere anche un ulteriore elemento di attenzione emergente dalla comunicazione congiunta sulle minacce ibride, vale a dire quello connesso ai rischi per l'uso delle sostanze chimiche, biologiche, radiologiche e nucleari, che costituisce materia specificatamente oggetto del piano d'azione dell'ottobre 2017 (COM(2017) 610 final) della Commissione.

Difatti il succitato documento prevede un pacchetto formato da ben 23 misure e azioni concrete volte a migliorare la protezione dei cittadini e delle infrastrutture critiche - inclusi gli aeroporti – nei confronti di queste minacce, anche attraverso una più forte cooperazione tra l'Unione europea e i suoi Stati membri.

Muovendo nel solco delle scelte internazionali in *subjecta materia*, preme segnalare che l'ICAO nel novembre 2017 ha inserito nel novero delle cinque priorità (involgenti 32 "azioni" e relativi 94 "compiti") del Global Aviation Security Plan (GASeP) una specifica attività imperniata sul primo capitolo "*enhance risk awareness and response*" e riferita proprio alla esigenza di identificare e affrontare la minaccia cyber nei confronti delle infrastrutture critiche, delle informazioni e dei sistemi tecnologici di comunicazione.

Orbene, giova soffermarci sul fatto che, in occasione dell'ultima Assemblea triennale, il predetto organismo ha altresì adottato una risoluzione (39/19) attraverso la quale invita gli Stati partner, l'industria e gli stakeholder ad intraprendere diversificate azioni mirate a combattere efficacemente le aggressioni cyber rivolte contro l'aviazione civile indicando, nel contempo, al Segretariato Generale di avviare ogni utile iniziativa acché le questioni di cybersecurity formino oggetto di coordinamento tra le diverse discipline seguite dall'ICAO e, di qui, sono stati successivamente istituiti numerosi gruppi tecnici di lavoro finalizzati a svolgere un'ampia gamma di interventi propositivi sulla problematica.

Non deve quindi sorprendere l'apprezzamento manifestato per la tematica di cui ci occupiamo in occasione della "Second - High Level Conference on Aviation Security" tenutasi a Montreal dal 29 al 30 novembre 2018, sotto l'egida dell'ICAO, ove si è discusso circa l'attuale potenzialità degli attacchi cyber non semplicemente perpetrati a livello nazionale ma anche riferibili su scala globale.

A conclusione poi dei lavori della conferenza è stato manifestato l'intento di promuovere lo sviluppo della Cybersecurity Strategy non disgiunta dai pertinenti meccanismi di identificazione e gestione del rischio, che contemplano la condivisione delle informazioni, nonché l'avvio di uno studio di fattibilità in seno all'Organizzazione per l'istituzione di un panel apposito per la Cybersecurity.

1) Si veda doc JOIN(2018) 14 final.
2) Si veda doc CMTD(2018)1228 del 28 novembre 2018.