G.E.O.



La strategia europea di contrasto al terrorismo

FOCUS SULL' AGENDA EUROPEA DEL 2020 E SULLA POLITICA UE IN MATERIA DI CONTRO-TERRORISMO.

REDATTO DA:

Cristiano Greco – Junior Researcher

Alessandra Fiorani – Senior Researcher

Mondo Internazionale
Associazione culturale
Gallarate, Via Marco Polo 31
21013 - VA, Italia
C.F. 91071700123
P.IVA 03727710125

Mail: segreteria@mondointernazionale.com

G.E.O. DIFESA E SICUREZZA

Analisi della strategia europea per la lotta al terrorismo: focus sull' agenda europea del 2020.

ABSTRACT

Al giorno d'oggi, il terrorismo costituisce una minaccia alla sicurezza nazionale, ai valori di democrazia e ai diritti e alle libertà fondamentali dei cittadini. La minaccia terroristica è uno dei pericoli attuali con cui gli Stati e le istituzioni internazionali devono confrontarsi quotidianamente. La lotta al terrorismo è una priorità assoluta per l'UE, gli Stati membri e i partner internazionali. La scelta di trattare i fenomeni terroristici è basata sulla rilevanza di questo fenomeno in materia di sicurezza nazionale.

Nella seguente trattazione si è cercato di fornire una panoramica completa e approfondita, andando ad indagare l'evoluzione del fenomeno terroristico dato l'avvento delle nuove tecnologie e di Internet. In primo luogo, si è scelto, di concentrare l'analisi sul territorio europeo allo scopo di indagare quali sono le recenti modalità di contrasto del fenomeno delineate dall'Unione Europea. Le linee guida strategiche da cui si è scelto di partire sono: l'Agenda contro-terrorismo per l'Europa, emanata in sede di Consiglio Europeo a dicembre 2020 e la relazione di EUROPOL sulla situazione terrorismo in Europa, che riporta di dati ufficiali in riferimento all'anno 2019. Nello specifico, l'Agenda è stata contemplata come fonte di riferimento da cui analizzare le misure antiterroristiche e per l'analisi descrittivo-qualitativa del fenomeno; di contro, il Report è stato il testo alla base dell'analisi quantitativa del fenomeno, grazie al quale è stato possibile estrapolare i dati utili alla corrente elaborazione.

In secondo luogo, vanno specificate le tipologie di terrorismo che si sono andate a trattare. La prima macro distinzione da fare è tra terrorismo nazionale e terrorismo internazionale. Con terrorismo domestico o nazionale si intende qualsiasi forma di terrorismo sviluppata da gruppi della stessa nazionalità del Paese- bersaglio nel quale operano e contro il quale operano. Invece, il terrorismo internazionale è il terrorismo operato da gruppi di nazionalità straniera rispetto al paese bersaglio, Paese colpito, nel quale operano. Rispetto alla seconda distinzione, va chiarito che non si tratterà solo di terrorismo di matrice jihadista, ma anche di forme di terrorismo basate sull'estremismo politico-ideologico, sia di destra che di sinistra. Si cercherà di mettere in relazione e in confronto le varie tipologie, estrapolando i loro tratti principali. L'indagine si svilupperà anche in riferimento al panorama italiano, andando ad analizzare le vicende del terrorismo domestico italiano attuato dai gruppi estremisti di sinistra.

INDICE

1. DATI DEL RAPPORTO EUROPOL SULL' ESTREMISMO DI SINISTRA
2. MOVIMENTI ANARCHICI E DI ESTREMA SINISTRA IN ITALIA
3. NUOVI MODI DI CONDURRE ATTACCHI TERRORISTICI
4. FINANZIAMENTO DEL TERRORISMO
5. CYBERTERRORISMO E LOTTA AI CONTENUTI ONLINE
6. PROTEZIONE DEGLI SPAZI PUBBLICI
7. RIABILITAZIONE E REINTEGRAZIONE DEI DETENUTI RADICALI
8. SCAMBIO INFORMATIVO E COOPERAZIONE INTERNAZIONALE

Conclusione

Glossario

Bibliografia

Sitografia



La strategia europea di contrasto al terrorismo

1. Dati del Rapporto Europol sull' estremismo di sinistra

In base ai dati forniti dal report dell'**Europol** sul terrorismo nell'UE del 2020, il numero (26) di attacchi commessi da movimenti di estrema sinistra e movimenti anarchici nel 2019 risulta in aumento rispetto ai due anni precedenti (24 nel 2017 e 19 nel 2018). I dati che, però, attirano l'attenzione sono quelli relativi al numero di arresti nel 2019 (111), il quale triplica il numero degli arresti nei due anni precedenti (36 nel 2017 e 34 nel 2018). Tra questi 111 arresti ben 98 sono stati segnalati dall'Italia, mentre i restanti sono stati segnalati dalla Grecia (4), dalla Spagna (8) e dall'Austria (1). La maggior parte degli arresti avvenuti in Italia (71) sono dovuti a scontri con la Polizia e dimostrazioni di protesta violente: 17 individui sono stati arrestati nel luglio 2019 per violenza contro le forze di polizia durante il G7 tenutosi a Taormina, nel settembre 2019 14 soggetti sono stati arrestati con l'accusa di condotta violenta durante alcune proteste a Torino e altre 14 persone sono state accusate di rivolta durante un evento tenutosi in Val di Susa a luglio.

I movimenti terroristi di sinistra agiscono in modo violento e seguono l'ideologia marxista-leninista col fine di scatenare una rivoluzione contro il sistema politico, sociale ed economico, introdurre il socialismo ed eventualmente stabilire una società comunista senza classi. Alcuni esempi di movimenti di estrema sinistra sono le italiane **Brigate Rosse** (BR) e la greca *Revolutionary Organisation 17 November.*

Terrorismo anarchico, invece, è un termine utilizzato per descrivere atti violenti commessi da gruppi o individui affiliati a diverse ideologie anarchiche. Gli anarchici promuovono un'agenda rivoluzionaria, anticapitalista e antiautoritaria. Esempi di queste organizzazioni sono l'italiana **Federazione Anarchica Informale** (FAI) e la greca *Synomosia Pyrinon tis Fotias* ("La Cospirazione delle cellule di fuoco).

Solitamente i movimenti terroristici di estrema sinistra e i movimenti anarchici rivendicano la responsabilità dei loro attacchi pubblicando dichiarazioni in lingua madre su alcune piattaforme pubbliche online affini alla loro ideologia. A volte vengono pubblicate anche dichiarazioni in inglese per raggiungere un pubblico internazionale.

In Italia, la minaccia più rilevante proviene dagli ambienti anarchici. La FAI si presenta come capillare e orizzontale, formata da individui e gruppi che apparentemente operano in autonomia sia in Italia che all'estero. I militanti italiani sono considerati un punto di riferimento per i membri stranieri, che aderiscono al **Fronte Rivoluzionario Internazionale** (FRI), operante principalmente in Grecia, Spagna e

Cile.

In Italia 22 attacchi (21 completati e 1 sventato) nel corso del 2019 sono stati attribuiti a movimenti di sinistra e gruppi anarchici e, nonostante, il numero di attacchi sia più che raddoppiato rispetto al 2018 (10), questi gruppi hanno mostrato una scarsa capacità operativa. La maggior parte degli attacchi risultano essere incendi dolosi (16 su 22) e gli obiettivi più frequenti sono veicoli appartenenti a compagnie pubbliche o private o ad agenzie governative. Anche i ripetitori televisivi e i cavi di telecomunicazione sono stati oggetto di attacchi, così come i cavi utili alla segnalazione dei treni e un tribunale. Un'esplosione IED[1] ha causato pochi danni a un edificio ospitante un'agenzia di collocamento a Rovereto e a Roma gli uffici di un partito di destra sono stati bersagliati dal lancio di un IID[2]. Le descrizioni di questi attacchi, spesso postate sul sito *roundrobin.info*, includevano manifestazioni di solidarietà verso tutti gli anarchici del globo detenuti in carcere e verso i rifugiati, manifestazioni di rifiuto di progetti infrastrutturali di vasta portata e dichiarazioni di ripudio della guerra.

Nel 2019 le attività dei movimenti anarchici sono risultate molto più estreme rispetto a quelle dei movimenti di estrema sinistra. Gli estremisti anarchici formano gruppi privi di struttura gerarchica che operano all'interno di specifiche aree urbane. Solitamente partecipano a proteste violente contro la Polizia o si infiltrano all'interno di manifestazioni non violente. **L'antifascismo, l'antirazzismo e la repressione statale** sono i temi più rilevanti della loro agenda. Oltre a questi vengono inclusi **l'antiglobalizzazione e l'anticapitalismo**, tant'è che molto spesso banche e compagnie multinazionali sono bersagli dei loro attacchi durante le proteste. Nell'ultimo anno anche le misure governative di contenimento al contagio hanno rappresentato uno spunto per questi movimenti. Sul web sono stati infatti condivisi diversi messaggi istigatori contro la "militarizzazione" del territorio e la volontà dello Stato di enfatizzare la pericolosità del virus per promuovere il controllo sociale[3].

Il conflitto scoppiato tra turchi e Curdi siriani nel 2019 risulta essere centrale nelle campagne di questi movimenti, tant'è che diversi militanti hanno deciso di viaggiare verso il Nord-Est della Siria, nel Rojava, per unirsi alle milizie curde. Il pericolo derivante dal ritorno di questi soggetti, che hanno acquistato esperienza partecipando al conflitto, diventa ora fonte di preoccupazione.

I movimenti anarchici e di estrema sinistra prediligono il Web per le attività di sensibilizzazione, di propaganda e di reclutamento e, vista la loro grande attenzione per la sicurezza, utilizzano telefoni "puliti" e applicazioni criptate per comunicare tra loro come ad esempio *Signal* e *Telegram.* Al contrario,

[1] Acronimo per "Improvised Explosive Device", indica una bomba realizzata con materiali non convenzionali

[2] Acronimo per "Improvised Incendiary Device", indica un ordigno progettato per creare incendi, piuttosto che creare un'esplosione

[3] "Relazione sulla politica dell'informazione per la sicurezza" del comparto intelligence (Dis, Aise e Aisi), 2020

alcuni gruppi preferiscono utilizzare metodi rudimentali, eliminando completamente l'utilizzo di computer e comunicazioni telefoniche, così come l'utilizzo di automobili e di GPS per i loro movimenti.

2. Movimenti anarchici e di estrema sinistra in Italia

I primi movimenti di estrema sinistra nacquero agli inizi degli anni 60 per iniziativa di nuclei di dissidenti della sinistra comunista e socialista e di intellettuali radicali marxisti che insorsero contro il riformismo della sinistra storica. I movimenti estremisti opponevano al riformismo e al revisionismo dei partiti ufficiali un ritorno alla teoria rivoluzionaria di Marx e Lenin.

Dall'unificazione di vari gruppi nel 1968 nasce a Milano l'organizzazione comunista **Avanguardia Operaia**, la quale fu uno dei gruppi più avanzati dal punto di vista dell'elaborazione teorica. Proponeva di creare il Partito rivoluzionario Marxista-Leninista, ma attraverso un processo graduale. Avanguardia Operaia poteva vantare forte legami con le lotte operaie grazie soprattutto all'egemonizzazione dei CUB, i **Comitati Unitari di Base**. Il gruppo non ha mai teorizzato né attuato atti di terrorismo e il suo contributo di violenza si è limitato agli scontri di piazza.

Altro gruppo significativo di estrema sinistra fu **Lotta Continua**, nato dalle ceneri de "Il Potere operaio di Pisa" su iniziativa del suo leader Adriano Sofri. Lotta Continua fu il gruppo più liberrario e più vicino alla scintilla movimentista del '68. Per Lotta Continua la violenza delle masse era la risposta naturale alla violenza interna del sistema borghese e, perciò fu spesso protagonista di scontri in piazza con la polizia, anche se al gruppo non fu mai attribuito alcun episodio di terrorismo.

La più importante e pericolosa organizzazione militante ed eversiva di sinistra fu quella delle Brigate Rosse (BR), le quali, tra il 1970 e il 1988, porteranno a termine diverse azioni terroristiche ai danni di persone e organizzazioni, causando decine di morti e seminando il terrore in tutto il paese. Lo scopo delle BR fu sempre politico, ossia sovvertire l'ordine democratico italiano attraverso la lotta armata, preparando la strada per una rivoluzione marxista. Le radici delle BR sono da ricercare negli ultimi anni '60, specificamente nell'autunno del 1969, ricordato come "l'autunno caldo", poiché protagonista di violenze molto intense, ma anche punto di svolta in cui gli operai abbandonarono i sindacati per affiliarsi a collettivi politici alternativi. I fondatori delle BR decisero di passare alla lotta armata durante alcuni incontri del **Collettivo Politico Metropolitano** (CPM), un gruppo milanese fondato da **Renato Curcio** e **Margherita "Mara" Cagol**.

Dopo la strage di Piazza Fontana, il CPM si trasforma in **Sinistra Proletaria** e verrà presa la decisione di adottare la lotta militare armata per ottenere potere politico ed educare le masse. Poco tempo dopo, sempre a Milano, nascono le BR. Esse dal punto di vista ideologico guardavano al Marxismo-Leninismo da una parte, e alla rivoluzione culturale maoista dall'altra. Secondo i loro piani la dittatura del proletariato sarebbe stata realizzata in 3 fasi: propaganda armata, attacco al cuore dello Stato e, infine,

una vera e propria guerra civile, che sarebbe culminata nel rovesciamento dello stato borghese. Dal punto di vista economico, le BR si finanziavano attraverso **rapine, rapimenti e riscatti** e, probabilmente, anche attraverso rapporti con paesi del blocco sovietico.

Dalla loro nascita fino al 1972 le BR prenderanno di mira le proprietà, più che le persone, quindi automobili, macchinari industriali e uffici. Le BR rivendicavano i loro attacchi attraverso volantini diffusi nelle fabbriche e spiegavano che le loro azioni erano punizioni per comportamenti che colpivano gli operai. Il primo sequestro targato BR avvenne nel marzo del 1972, quando l'ingegnere della Sit-Siemens, **Idalgo Macchiarini**, viene sequestrato e fotografato con un cartello al collo sul quale vi era scritta una frase di Mao Tse-Tung "colpiscine uno per educarne cento", e poi liberato nella stessa giornata. I sequestri continuarono e tra il 1973 e il 1974 si diede inizio **all'attacco al cuore dello Stato**, una fase in cui le BR porteranno avanti diverse azioni in grado di incidere sulla politica nazionale, attaccando direttamente lo Stato italiano.

Dopo una serie di arresti, tra cui quello di Renato Curcio, e la morte di "Mara" Cagol, le BR, nel 1976, si trasformano in un'organizzazione di guerriglia. Il 1978 è l'anno del **sequestro Moro**, il punto più alto della sfida violenta allo Stato lanciata dalle BR. Da allora, però, inizia anche il declino del gruppo. Diversi membri delle BR iniziavano a cooperare con la giustizia e il gruppo si frammentava in più correnti fino a quando alla fine degli anni 80 il movimento storico fu dichiarato sostanzialmente finito.

Per quanto riguarda il movimento anarchico italiano, esso ha una lunga storia che parte dal Risorgimento, con la nascita di Fratellanza Internazionale nel 1864, e arriva fino ai giorni nostri con la salita alla ribalta della Federazione Anarchica Informale (FAI). Proprio la FAI viene citata più volte nel report di Europol, poiché considerata una delle più importanti a livello europeo e anche globale. Essa nasce nel 2003 con la rivendicazione dell'esplosione avvenuta nei pressi della casa bolognese di Romano Prodi.

La FAI è un movimento rivoluzionario con una struttura orizzontale, composta da vari gruppi uniti in un patto federativo di mutuo appoggio, il quale è incentrato su 3 punti chiave: solidarietà, campagne rivoluzionarie e comunicazione tra gruppi e singoli. La federazione si definisce[4] anarchica perché punta alla distruzione dello Stato e del capitale ed informale perché priva di meccanismi autoritari e burocratizzanti. Ciò permette di garantire l'anonimato e l'indipendenza dei gruppi e degli individui che la compongono.

Grazie ad Internet, la FAI ha fatto conoscere le sue idee e contemporaneamente è venuta a conoscenza delle attività di gruppi non italiani. La diffusione dei comunicati sul Web ha quindi aperto la strada alla costruzione del Fronte Rivoluzionario Internazionale, una federazione di gruppi anarchici affini.

[4] http://apa.online.free.fr/article.php3?id_article=243

Nel 2012 si è verificato un salto di qualità nelle azioni della FAI. Per la prima volta, infatti, i militanti della Federazione avevano sparato una persona, precisamente **Roberto Adinolfi**, direttore generale di Ansaldo Nucleare, una compagnia operante nel settore nucleare controllata da Finmeccanica. Adinolfi venne sparato al ginocchio e quindi non con la finalità di uccidere, ma l'attacco rievocò le paure del terrorismo, dal momento che le gambizzazioni erano un marchio di fabbrica delle BR. Tra il 2012 e il 2013 le autorità italiane hanno provveduto all'arresto di diversi anarchici, e dopo tale ondata di arresti l'intelligence italiana ha dichiarato la FAI, momentaneamente, in un periodo di stallo operativo. Ciononostante, la minaccia derivante dai network anarchici rimane elevata come dimostrato dal report di Europol.

3. Nuovi modi di condurre attacchi terroristici

Nell'Agenda Controterrorismo Europea del 2020 si afferma che: *"la natura degli attacchi sta cambiando*". L'Ue deve saper fronteggiare le minacce terroristiche provenienti dalle nuove tecnologie e dai nuovi modi di condurre questa tipologia di attacchi, per esempio tramite: l'uso malevolo di droni, l'intelligenza artificiale, e materiale chimico, biologico, radiologico e nucleare. Partendo da queste considerazioni, il capitolo corrente si propone lo scopo di indagare la natura di queste sofisticate armi e l'utilizzo che ne derivano i gruppi terroristici, si partirà dalle tipologie di armi "tradizionali" per arrivare all'impiego delle moderne tecnologie.

L'uso di armi esplosive ed incendiarie.

In accordo con il *Report* sulla situazione europea di EUROPOL in materia di terrorismo, l'uso di esplosivi rappresenta tutt'ora un mezzo privilegiato per condurre gli attacchi terroristici di due categorie specifiche: i gruppi etno-nazionalisti/ separatisti e quelli estremisti di destra. Rispetto al terrorismo di matrice jihadista, si è notato un incremento dell'interesse nell'uso di armi esplosive, anche se negli attacchi perpetrati da *foreign fighter* e lupi solitari l'arma bianca continua ad essere la prima scelta.
Con riguardo al terrorismo di sinistra, invece, si sono continuati ad utilizzare dispositivi esplosivi e incendiari rudimentali e improvvisati, nello specifico usati per causare danni ad edifici, reti dei servizi essenziali e beni pubblici. Questo incremento nella fabbricazione fai-da-te degli esplosivi è stato favorito dal libero accesso a piattaforme online specializzate, difatti EUROPOL scrive che "*nel 2019 è stato notato l'aumento del volume di materiale online che incitava ad attacchi incendiari solitari*"[5]. Si

[5] *EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2020,* EUROPOL- European Union Agency for Law Enforcement Cooperation, 2020, pag.19.

può evidenziare come il perossido di acetone si conferma uno dei principali esplosivi fabbricati in casa, tant'è che viene comunemente chiamato "l'esplosivo degli attentatori": uno dei più dannosi materiali esplosivi che può essere preparato in laboratori rudimentali, è estremamente sensibile alle fiamme, per cui basta un semplice involucro di carta stagnola per provocare l'effetto detonatore[6].

Per ultimo, rispetto le armi incendiarie, non sono da sottovalutare le azioni di propaganda online per cui EUROPOL ha registrato un significativo aumento dei contenuti incitanti gli attori solitari a condurre attacchi tramite incendi dolosi. Di certo un trend che ad oggi ha avuto ben poca rilevanza ma che in futuro potrebbe rappresentare un mezzo efficace e poco dispendioso per perpetrare tali azioni terroristiche.

Armi chimiche, biologiche, radiologiche e nucleari.

In questa macrocategoria di armi rientrano quei mezzi che hanno la capacità, almeno potenziale, di arrecare una quantità di danni decisamente superiore a qualsiasi altro dispositivo, per questo vengono anche dette "armi di distruzioni di massa"[7].All'interno di questa ampia definizione abbiamo varie tipologie di armi, appunto: chimiche, biologiche, radiologiche e nucleari.
Nel Report di EUROPOL tra i trend del 2019 non si evidenzia alcune significativo aumento dell'uso di questi dispositivi per l'attuazione di attacchi terroristici. Gli elementi preoccupanti però sono ben due:

1- Il primo di minor allarme, cioè l'uso dei fertilizzanti, materiali pirotecnici e altre sostanze chimiche per la fabbricazione di armi esplosive;

2- Quest'ultimo di maggior rilevanza, per cui nel 2019 sono stati intercettati dei contenuti online riconducibili a gruppi terroristici di matrice islamica, in cui si incitava all'uso di armi biologiche. Nello specifico venivano illustrate le istruzioni per produrre tali strumenti e per il successivo posizionamento e utilizzo.

Similmente, non sono stati ancora effettuati attentati tramite i materiali nucleari e radioattivi, anche se suddette armi continuano ad essere una preoccupazione globale di lunga data.

L'armamento dell'Intelligenza Artificiale.

[6] *TACTP o perossido di acetone: quali criticità per l'intervento operativo degli specialisti;* Scaini Stefano / Auddino Lorenzo / Canfarini Federico; Analytica for intelligence and security studies- Paper Crisis Management; 2020.
[7] *LE ARMI DI DISTRUZIONE DI MASSA*; Stefano Felician; CASD; Ministero della Difesa.

Il terrorismo, nell'era della tecnologia, non può non aver considerato l'utilizzo dell'*Artificial Intelligence* a proprio favore. Tuttavia ad oggi, non sussistono casi reali di attacchi terroristici in cui l'AI viene convertita ad arma. Di contro è innegabile lo sviluppo dell'impiego di queste intelligenze in ambito militare, anche tramite l'applicazione di queste capacità ai dispositivi militari convenzionali. Se ciò che si è verificato per la tecnologia GPS, nata per l'utilizzo militare e poi integrata nei comuni dispositivi civili, vale anche per l'intelligenza artificiale, non appare infondato preoccuparsi del loro- possibile- uso improprio.

L'ipotesi più plausibile per cui i dispositivi militari a cui sono state applicate forme di AI possano cadere in mano ad organizzazioni terroristiche si basa sull'uso che gli Stati fragili ne fanno. Attualmente i principali acquirenti di dispositivi con tecnologie AI sono gli Stati. Gli strumenti e la tecnologia dell'IA vengono impiegati e sviluppati da Paesi che potrebbero non usarli all'interno delle logiche del diritto internazionale. Data la fragilità di questi Stati, un loro collasso o rovescio di regime al loro interno, potrebbe facilitare l'acquisizione di potere dei gruppi terroristici e, di seguito, anche la possibilità che l'AI applicata alle armi entri in loro possesso. Gli scopi per cui i terroristi potrebbero impiegare queste tecnologie sono per la preparazione delle loro operazioni; per la raccolta di informazioni; per le campagne di propaganda e informazione e, infine, per la ricognizione. Come ultima ipotesi si riporta la possibilità di applicare l'AI ai robot per uso maligno*,* in gergo *"robot killer"*. Anch'essi dispositivi nati in ambito militare come armi autonome e letali, in grado di individuare il bersaglio da colpire e procedere all'attacco. Quest'ultima risulta essere una prospettiva accattivante per le organizzazioni terroristiche ma assolutamente estrema.

La minaccia posta dai droni.

I droni sono "aeromobili a pilotaggio remoto" (APR) difatti si caratterizzano per essere dei velivoli radiocomandati con guida da remoto utilizzati sia in ambiti professionali, civili e militari. Grazie alle caratteristiche di questo dispositivo la loro applicazione ha spaziato nei più disparati usi civili, tant'è che esistono delle categorie di "droni commerciali". Dato il loro prezzo accessibile ai più e le misure ridotte – per cui esistono anche dei prototipi di "mini droni" - essi si sono trasformati in una perfetta arma con possibilità di modifica.

Gli elementi che rendono questo aeromobile interessante per i civili e di conseguenza anche per i gruppi terroristici sono:

- le dimensioni e il peso;
- la capacità di elevazione, cioè l'altezza dal suolo che può raggiungere;
- l'autonomia o meglio la durata della batteria;

- i sistemi per il controllo e il pilotaggio remoto, in base alla tecnologia con cui vengono pilotati si determina anche la variazione del raggio d'azione. Ad esempio: i droni comandati tramite Bluetooth supportano un raggio d'azione che va dai 10 ai 20 metri; quelli tramite Wi-Fi prevedono un raggio d'azione massimo di 50 metri; per ultimi i droni comandati con sistemi di radiofrequenza per cui si possono raggiungere anche chilometri e sono tipici dei droni professionali.
- la capacità di volteggio ed acrobazie;
- la telecamera di supporto; i droni dotati di questo supporto come videocamera o fotocamera sono utili per ricognizione e attività di acquisizione delle immagini di un settore bersaglio.
- GPS, di cui sono dotati generalmente di droni professionali.

Inoltre le ragioni per cui i gruppi terroristici stanno frequentemente ricorrendo ai droni sono da ricercare nella loro facilità di acquisto e reperimento tramite siti di e-commerce online. Questa considerazione apre uno spunto di riflessione sul fatto che la vendita di questi strumenti non è ancora regolamentata.

Si potrebbe ingenuamente credere che i droni professionali siano i più richiesti da questi gruppi, in realtà le dimensioni dei "mini droni" li rendono un'arma perfetta. Questa categoria di droni è difficilmente identificabile e si caratterizza per essere invisibile ai radar, inoltre, una volta che sono in volo, sono difficilmente visibili anche all'occhio umano.
Già accennata in precedenza, la facilità di modifica rende possibile la trasformazione in armi in molteplici modi. Per esempio, online sono facilmente reperibili guide e spunti per sostituire la fotocamera con dell'esplosivo, in tal modo si trasforma lo strumento in un drone suicida.
Non è da escludere, inoltre, l'utilizzo dei droni per azioni di propaganda tramite le immagini degli attacchi registrate dal supporto video del velivolo.
Per ultima, così come l'ipotesi dei *robot killer*, ritorna anche l'idea di "*sciami di droni killer*". Lo scenario di "sciami di droni assassini" è collegato alla prova che l'ISIS ha usato sul campo di battaglia siriano piccoli droni di consumo armati di granate, oppure all'ipotesi per cui droni dotati di intelligenza artificiali vengono programmati per effettuare uccisioni mirate.[8]

L'uso di stampanti 3D.

[8] Fonti nella scrittura di questo paragrafo: https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology/ ; https://www.agendadigitale.eu/sicurezza/droni-civili-a-scopo-offensivo-problemi-e-soluzioni/

L'ultima parte della trattazione dedicata all'uso delle tecnologie come mezzi per compiere attentati terroristici, va ad indagare l'utilizzo delle stampanti 3d come ausilio per fabbricare armi fatte in casa. Dopo la vicenda dell'attentato di Halle, in Germania, ad opera di un esponente di estrema destra nei confronti di una sinagoga è stato appurato che l'attentatore aveva usato una pistola fatta in. Parti della pistola sono state presumibilmente stampate utilizzando una stampante 3D.
Questa possibilità appare un'ipotesi assolutamente plausibile data la facilità di reperimento online dei manuali di fabbricazione delle armi da fuoco e un'altrettanta agevolezza nell'acquisto online di stampanti 3D. In sostanza dato che la qualità della stampa 3D sta subendo uno sviluppo tecnologico e l'incremento dell'accessibilità a contenuti online, il rischio e l'efficacia dei terroristi che costruiscono le proprie pistole probabilmente aumenteranno ulteriormente.

L'analisi dei fatti dell'attentato di Halle ci torna però utile per introdurre il prossimo argomento tramite cui si intende indagare il fenomeno terroristico. La vicenda si è svolta martedì' 8 ottobre 2019 nella città di Halle, nell'est della Germania. Il giorno scelto per l'attacco ricordava la guerra dello Yom Kippur, una festa di tradizione ebraica. L'obiettivo dell'attacco è stata una sinagoga e sono rimasti vittime due civili. Al di là delle motivazioni che hanno spinto l'attentatore, che come riportato sopra si identifica nel terrorismo di estrema destra, ciò che ci interessa ai fini della presente trattazione è la volontà del soggetto di trasmettere in diretta quello che stava facendo. La testimonianza del suo operato è stata riportata in diretta tramite una piattaforma di videogiochi online- *Twitch.* Il video, prima di essere rimosso, ha circolato nel web e si stima abbia avuto circa duemila visualizzazioni. Questo elemento sempre più frequente nell'operato dei terroristi rimanda la riflessione al paragrafo 5: la propaganda online, il cyberterrorismo e il contrasto a questi contenuti.

4. Finanziamento Del Terrorismo

Con finanziamento al terrorismo si intende quell'insieme di attività poste in essere al fine di reperire denaro o altri supporti, anche materiali, in favore delle organizzazioni terroristiche. La prima definizione di finanziamento al terrorismo si rinviene nell'articolo 2 della Convenzione di New York del 1999, che inquadra questo fenomeno come un'attività di fornitura di fondi e risorse economiche, caratterizzata da un aspetto oggettivo, ossia il fornire fondi con qualsiasi mezzo, e da un aspetto soggettivo, relativo alla consapevolezza che tali fondi saranno utilizzati per svolgere azioni illecite con la finalità di intimidire una popolazione o obbligare un governo o un'organizzazione internazionale a compiere o ad astenersi dal compiere qualcosa. Questa prima definizione di terrorismo è stata poi resa più chiara nella risoluzione del Consiglio di sicurezza ONU n.1373/2001 e nelle raccomandazioni

della Financial Action Task Force. Nella nuova definizione veniva eliminato l'elemento soggettivo della volontà di finanziare atti terroristici, considerando il finanziatore sempre responsabile anche nel caso in cui i fondi venissero destinati non a un atto terroristico, ma all'organizzazione in toto.

A livello europeo, il finanziamento al terrorismo trova la sua prima collocazione nella posizione comune del Consiglio n.931/2001, relativa all'applicazione di determinate misure per combattere il terrorismo, e nella decisione del Consiglio n. 475/2002, che puniva le condotte di partecipazione in un gruppo terroristico.

L'attività di riciclaggio è strettamente connessa al finanziamento del terrorismo. Il riciclaggio di denaro segue un processo ben preciso, composto da un ampio numero di transazioni e da un ampio numero di strutture finanziarie coinvolte. Quest'attività si articola in 3 fasi: il *placement*, in cui il denaro di provenienza illecita viene collocato in un istituto finanziario; il *laundering*, durante il quale vengono occultate le origini illecite di tale denaro e la sua proprietà; l'*integration,* momento in cui il denaro ripulito viene immesso nel circuito economico legale. L'intreccio tra il finanziamento al terrorismo e il riciclaggio è molto chiaro, considerando che il finanziamento al terrorismo può costituire reato presupposto del riciclaggio, e il riciclaggio risulta un prezioso strumento per le associazioni terroristiche per ripulire il denaro acquisito illecitamente e reinvestirlo nel circuito economico, occultandone del tutto la provenienza.

Tra le istituzioni europee è la Commissione ad essere fortemente impegnata nella lotta contro il riciclaggio e il finanziamento del terrorismo, sia a livello europeo che a livello globale. I rischi legati al riciclaggio e al finanziamento del terrorismo costituiscono, infatti, una grave minaccia per il sistema finanziario dell'UE e la sicurezza dei suoi cittadini.

L'UE, negli ultimi decenni, ha elaborato un solido quadro normativo per prevenire e combattere il riciclaggio di denaro e il finanziamento del terrorismo, definiti dalla Corte di Giustizia dell'UE come questioni di protezione dell'ordine pubblico. Le norme europee devono essere, tuttavia, costantemente adattate per tenere conto dei rischi derivanti dalle innovazioni tecnologiche, come ad esempio le valute virtuali, dalla crescente integrazione dei flussi finanziari nel mercato interno, dalla globalizzazione delle organizzazioni terroristiche e dall'ingegnosità dei criminali nello sfruttare le lacune del sistema. Per raggiungere tale risultato viene richiesta una forte cooperazione a livello internazionale. L'UE, a tal proposito, collabora con i partner del Gruppo di azione finanziaria internazionale (GAFI)[9] al fine di elaborare e attuare norme internazionali. I recenti sviluppi in ambito

[9] Il Gruppo di azione finanziaria internazionale è l'organismo internazionale incaricato di definire le norme in questo settore. Istituito nel 1989, è un task force intergovernativa che sviluppa e promuove politiche contro il riciclaggio di denaro e il finanziamento del terrorismo e formula raccomandazioni che i Paesi sono tenuti a seguire. Ne fanno parte la Commissione Europea e 14 Stati Membri dell'UE. Altri Stati Membri dell'UE fanno parte di Moneyval, un organismo regionale analogo al

legislativo hanno avuto per obiettivo il rafforzamento del quadro dell'UE in materia di lotta al riciclaggio di denaro e al finanziamento del terrorismo (AML/CFT). A tal riguardo si potrebbero citare la quinta direttiva antiriciclaggio[10] entrata in vigore nel giugno 2018 che mira a migliorare la trasparenza riguardo alla titolarità delle società e dei trust, a rafforzare i controlli sui paesi terzi a rischio, a rafforzare la cooperazione tra unità nazionali di informazione finanziaria e a migliorare la cooperazione tra le autorità di vigilanza antiriciclaggio e la BCE. Inoltre, si possono ricordare il rafforzamento del mandato dell'Autorità bancaria europea [11], le nuove disposizioni che si applicheranno ai controlli sul denaro contante a partire dal giugno 2021 e una definizione armonizzata dei reati e delle sanzioni relativi al riciclaggio di denaro.

Al fine di garantire una politica organica dell'UE in materia di prevenzione del riciclaggio di denaro e di lotta al finanziamento del terrorismo, la Commissione, attraverso la comunicazione "Verso una migliore attuazione del quadro dell'Unione in materia di lotta la riciclaggio di denaro e al finanziamento del terrorismo"[12] ha stabilito delle misure necessarie da intraprendere. Tra esse figurano un corpus normativo più dettagliato e armonizzato, una vigilanza coerente e di alta qualità da implementare attraverso un organismo di vigilanza europeo che agisca in cooperazione con le autorità nazionali competenti, e un meccanismo rafforzato per coordinare e sostenere l'operato delle unità d'informazione finanziaria che consentirebbe un accesso transfrontaliero più rapido alle informazioni sui conti bancari da parte delle autorità di contrasto. Tali misure favorirebbero l'integrità del sistema finanziario e, di conseguenza, risulterebbero fondamentali per il completamento dell'Unione bancaria e dell'Unione economica e monetaria.

Per quanto riguarda il rafforzamento della vigilanza, come evidenziato dal pacchetto antiriciclaggio del luglio 2019[13], risulta necessario superare le significative carenze nella gestione del rischio da parte degli enti creditizi e nella loro sorveglianza. Un sistema di vigilanza integrato permetterebbe di affrontare il problema della frammentazione della vigilanza e garantirebbe l'attuazione armonizzata delle norme in materia di AML/CFT, senza però sminuire l'importanza delle autorità di vigilanza nazionali che resterebbero fondamentali nella vigilanza quotidiana.

GAFI. Le raccomandazioni del GAFI sono attuate nell'UE attraverso la quinta direttiva antiriciclaggio.

[10] Direttiva UE 2018/843

[11] Regolamento UE 2019/2175

[12] COM (2019) 360 final

[13] Il pacchetto antiriciclaggio della Commissione, adottato il 24 luglio 2019, è costituito da una comunicazione politica dal titolo "Verso una migliore attuazione del quadro dell'Unione in materia di lotta al riciclaggio di denaro e al finanziamento del terrorismo"(COM (2019) 360), dalla relazione sulla valutazione di recenti presunti casi di riciclaggio di denaro concernenti enti creditizi dell'UE ("post mortem") (COM (2019) 373), dalla relazione sulla valutazione dei rischi di riciclaggio e finanziamento del terrorismo che incidono sul mercato interno e sono connessi ad attività transfrontaliere (la relazione sulla valutazione sovranazionale del rischio (RVSR)) (COM (2019) 370) e il relativo documento di lavoro dei servizi (SWD (2019) 650), e dalla relazione sull'interconnessione dei meccanismi nazionali centralizzati automatici (registri centrali o sistemi elettronici centrali di reperimento dei dati) degli Stati membri relativi ai conti bancari (COM (2019) 372)

Il mandato dell'autorità di vigilanza europea dovrebbe coprire tutte le aree di rischio ed essa dovrebbe disporre di tutti gli strumenti necessari per armonizzare le pratiche all'interno dell'UE. Al momento sono al vaglio anche altre opzioni con un ambito di applicazione più limitato, come ad esempio il solo controllo delle istituzioni finanziarie, che garantirebbe una vigilanza più agevole, ma non consentirebbe di istituire un sistema efficace di lotta al riciclaggio e al finanziamento del terrorismo.

Non è ancora ben chiaro quale organo dell'UE verrebbe investito di tale compito, ma le alternative sembrano essere due al momento: assegnarlo a un'agenzia europea già esistente, ossia **l'Autorità Bancaria Europea** (ABE), o a un nuovo organismo istituito ad hoc.

Assegnare all'ABE responsabilità di vigilanza in materia di AML/CFT presenterebbe vantaggi per quanto riguarda la continuità e la rapidità d'intervento. Questa opzione richiederebbe, però, una riforma profonda dell'ABE e un significativo sviluppo delle conoscenze e delle competenze in materia di AML/CFT. Andrebbero rivisti la governance e i processi decisionali e dovrebbero essere rafforzati la sua capacità e i suoi poteri d'indagine.

Nel caso in cui venisse istituito un organismo ad hoc, potrebbe essere messo a punto un sistema su misura in termini di organizzazione e governance, con processi decisionali semplificati e rapidi per reagire velocemente ai rischi. Per rendere operativo un nuovo organismo, tuttavia, potrebbe essere necessario più tempo e i costi sarebbero più elevati.

Altro punto al centro del dibattito è l'istituzione di un meccanismo di coordinamento e di sostegno delle unità d'informazione finanziaria a livello europeo, il quale permetterebbe di ovviare alle carenze riguardanti lo scambio limitato di informazioni tra le unità d'informazione finanziaria e le altre autorità competenti. Il meccanismo sarebbe utile nell'individuazione di transazioni sospette con dimensione transfrontaliera, nell'analisi congiunta dei casi transfrontalieri e nell'individuazione delle tendenze e dei fattori pertinenti per valutare i rischi di riciclaggio di denaro e di finanziamento del terrorismo a livello nazionale e sovranazionale. Il meccanismo dovrebbe, inoltre, adottare o proporre norme d'esecuzione e promuovere la formazione e lo sviluppo di capacità per le unità d'informazione finanziaria, e rafforzerebbe la cooperazione tra le autorità competenti e con le unità d'informazione finanziaria al di fuori dell'UE. In questo contesto è inoltre rilevante investire nella rete **FIU.net**, il sistema europeo per lo scambio d'informazioni tra le unità d'informazione finanziaria, per superare i problemi che ostacolano lo scambio d'informazioni e la verifica della corrispondenza dei dati.

La Commissione ritiene, inoltre, che il **Centro europeo per la criminalità finanziaria ed economica** (EFCEC) guidato dall'Europol potrebbe fungere da naturale controparte del meccanismo di sostegno e coordinamento dell'UE per le unità d'informazione finanziaria. Il centro permetterà di concentrare in un unico organismo tutte le capacità di Europol per il contrasto della criminalità economica e

finanziaria e cercherà di rafforzare l'efficacia di intervento, aumentare la visibilità operativa e migliorare la gestione dei portatori di interessi e le opportunità di finanziamento.

Al fine di migliorare le attività investigative e l'azione penale nei casi di riciclaggio di denaro in tutta l'UE, la Commissione finanzia anche la rete operativa contro il riciclaggio di denaro (AMON) che mette in collegamento le pertinenti autorità di contrasto e facilita le indagini finanziarie transfrontaliere, visto il suo carattere globale. Gli Stati membri, inoltre, dovrebbero continuare ad avvalersi del sostegno di Eurojust per agevolare la cooperazione transfrontaliera a sostegno dei procedimenti giudiziari contro il riciclaggio di denaro. Il perfezionamento delle attività investigative passa anche dall'istituzione di nuove strutture come la Procura europea, entrata in funzione nel settembre scorso, che si occuperà dell'indagine e del perseguimento dei reati commessi dalla criminalità finanziaria transnazionale, o la creazione di un network di investigatori finanziari con compiti di controterrorismo come proposto dalla Commissione. Infine, a proposito di investigazione finanziaria, bisogna citare il *Terrorist Finance Tracking Programme* (TFTP), un programma che, attraverso il tracciamento dei flussi monetari, ha consentito la scoperta di diverse cellule terroristiche.

Nel contesto di un migliore utilizzo dell'intelligence finanziaria, dovrebbe inoltre essere promosso nella misura del possibile il ruolo dei partenariati pubblico-privato, i quali prevederebbero la condivisione delle informazioni tra le autorità di contrasto, le unità di informazione finanziaria e il settore privato.

Come si finanziano i terroristi?

Negli anni le organizzazioni terroristiche hanno sviluppato tecniche sempre più avanzate per ottenere risorse. Secondo i dati della Financial Action Task Force (FATF), le risorse dell'ISIS hanno da un lato una provenienza indiretta, in quanto derivanti dalle donazioni di supporters anonimi, dagli Stati sponsor o da associazioni di beneficienza, ma dall'altro lato vengono ottenute direttamente dai terroristi, i quali cercano di dotarsi di fonti autonome quali la gestione di giacimenti petroliferi, la richiesta di fondi ad altri gruppi terroristici e le zakat, ovvero donazioni ai quali i Musulmani sarebbero tenuti per purificare le loro anime.

Analizzando i metodi di finanziamento, non è possibile tralasciare l'importanza delle nuove tecnologie. Lo sviluppo tecnologico, in particolare la dematerializzazione della moneta, costituisce, infatti, un forte vantaggio per i gruppi terroristici, poiché permette di svolgere transazioni anonime difficili da controllare. Le valute virtuali sono oggi uno dei principali strumenti utilizzati dal terrorismo per mascherare l'origine illecita dei capitali. L'autorità bancaria europea ha definito le valute virtuali "a form of unregulated digital money, not issued or guaranteed by a central bank, which can act as means of payment"[14].

[14] https://www.eba.europa.eu/eba-warns-consumers-on-virtual-currencies

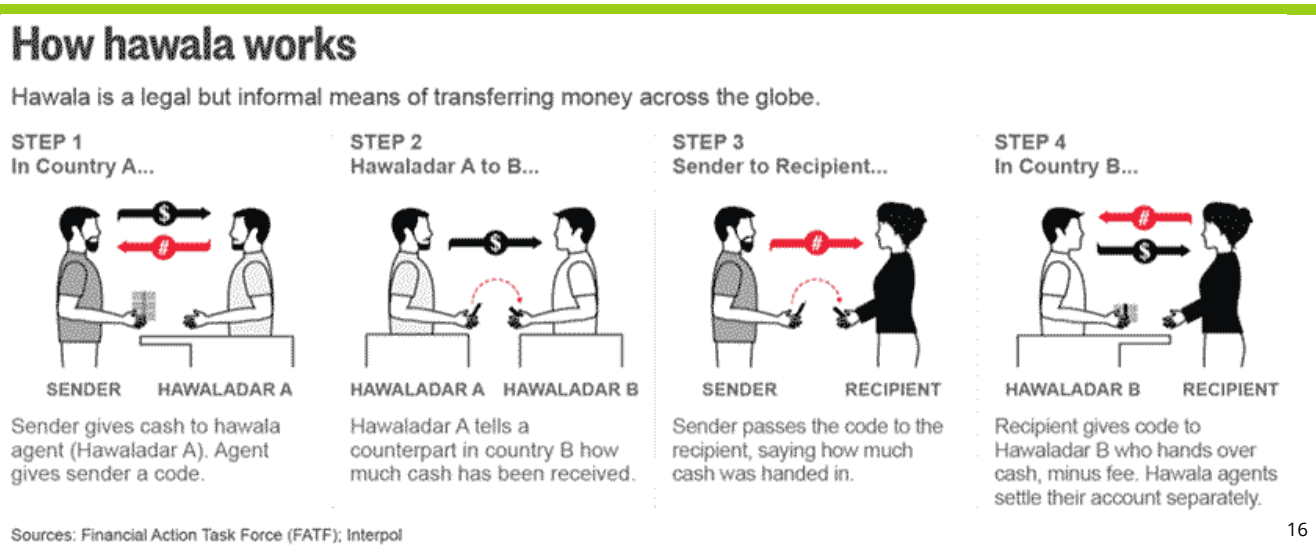
Le cellule terroristiche e gli individui facenti parte di organizzazioni terroristiche non hanno bisogno di mantenere un'infrastruttura per finanziarsi. Il Belgio ha osservato che le cellule in Europa si finanziano attraverso **piccoli crimini, furti ed estorsioni**, mentre gli apparati stanziati nel Medio Oriente ricevono finanziamenti grazie alle **donazioni** di simpatizzanti jihadisti. C'è anche la possibilità che parte dei proventi derivanti dall'agevolazione dell'immigrazione illegale siano utilizzati per finanziare il terrorismo. Nel maggio 2019, a tal proposito, 4 cittadini somali sono stati arrestati in Italia poiché sospettati di raccogliere denaro nei luoghi di culto per fini terroristici. I fondi, infatti, sarebbero stati utilizzati per finanziare le attività terroristiche somale e anche per promuovere l'immigrazione irregolare verso l'Italia.

Le organizzazioni clandestine attive fuori dall'Europa utilizzano questi fondi, inclusi quelli generati in Europa, per stabilire servizi finanziari e sociali nelle aree sotto il loro controllo. Col tempo, tuttavia, la portata dei finanziamenti risulta essere in diminuzione viste le grandi perdite di territori tra Iraq e Siria precedentemente in mano allo Stato Islamico.

I trasferimenti di denaro vengono eseguiti attraverso diversi canali, ma principalmente attraverso l'*hawala* o attività bancarie clandestine. L'*hawala* è, secondo la definizione della Commissione[15], un *informal value transfer service* che costituisce una minaccia nel contesto del finanziamento al terrorismo. *Hawala* è una parola araba che significa "scambiare" e indica un sistema alternativo ben radicato nella cultura islamica e basato sulla fiducia, che trova fondamento nei testi della giurisprudenza islamica dell'VIII secolo. Questo sistema è nato per trasferire fondi legittimi e con finalità lecite al fine di eliminare del tutto il rischio derivante dal trasporto internazionale delle valute, e risulta essere efficace poiché permette di muovere denaro in modo veloce ed economico e senza coinvolgere le istituzioni finanziarie.

La *hawala* è caratterizzata dalla presenza di due agenti chiamati *hawaladar*. Il primo si trova nel luogo di partenza del denaro e l'altro nel luogo di ricezione. Ad essi si rivolgono sia il cliente che vuole trasferire il denaro sia il beneficiario.

[15] COM (2017) 340 final



16

Come dimostrato dall'immagine sono 4 i passaggi che portano il denaro dal cliente al beneficiario:

1. Il cliente per trasferire i soldi nel paese dell'*halawadar* B si rivolge all'*hawaladar* A, con il quale concorderà le commissioni applicate sulla transazione e l'eventuale tasso di cambio, applicato qualora il trasferimento avvenisse in due valute differenti; l'*hawaladar* A in seguito alla transazione consegnerà un codice al cliente;
2. L'*hawaladar* A contatta l'*hawaladar* B informandolo dei dettagli dell'operazione e gli comunica la stessa parola d'ordine che dovrà essere comunicata dal beneficiario nell'ultima fase;
3. Il cliente passa il codice al beneficiario, specificando la somma di denaro consegnata;
4. L'*halawadar* B, dopo avere ricevuto il codice da parte del beneficiario, trasferisce i soldi a quest'ultimo; i due *hawaladar* regolano successivamente le partite di debito e credito separatamente

L'efficacia e l'efficienza dell'*hawala* è dovuta a diversi fattori, quali la velocità (operazioni concluse in 24 ore), l'economicità (le commissioni richieste dall'*hawaladar* sono molto più basse rispetto a quelle richieste nei circuiti convenzionali), l'anonimato, la versatilità e l'affidabilità.

Per quanto riguarda la figura dell'*hawaladar*, bisogna specificare che spesso è un piccolo imprenditore del settore import/export. L'integrazione dell'*hawaladar* nelle attività lecite gli permette di generare cassa per le operazioni giornaliere di *hawala*, di accordarsi con clienti provenienti da altri paesi così da farli diventare *hawaladar* e di trovare nuovi clienti attraverso l'attività ufficiale.

[16] https://thestandrewseconomist.com/2019/12/28/the-hawala-system-and-sharia-banking/comment-page-1/

5. Cyberterrorismo e lotta ai contenuti online.

Definire il cyberterrorismo non è un'attività semplice per via della mancanza di una definizione univoca e universalmente riconosciuta e a causa delle molteplicità tentativi accademici. Generalmente, con il termine *cyberterrorismo* si intende l'insieme delle azioni, perpetrate nel cyberspazio, ideologicamente motivate volte a condizionare uno Stato o un'organizzazione internazionale. Secondo il Rapporto sulla situazione del terrorismo del 2012 redatto da EUROPO, il termine cyberterrorismo *"is used variously to describe activities including electronic attacks on critical infrastructure, intellectual property theft relating to research and development, and even the use of Internet technology for the dissemination of propaganda or for communication purposes*"[17]. Grazie a questo tentativo di esplicazione del nuovo fenomeno terroristico, è possibile riscontrare due diversi significati: nella prima concezione del fenomeno vi rientra l'approccio *target oriented* per cui la rete è intesa come obiettivo da colpire e nello stesso tempo come arma di cui servirsi. Secondo questo paradigma le organizzazioni terroristiche o i lupi solitari utilizzano il web sia per danneggiare e compromettere i sistemi informatici di un Paese-target, sia come arma tramite cui perpetrare attacchi informatici.

Nel secondo significato, invece, vi rientra l'approccio *tool oriented* in cui la rete è intesa principalmente come strumento e come supporto per portare a termine l'attacco. All'interno di questo secondo approccio vi rientrano varie attività deputate allo sviluppo e sopravvivenza dell'organizzazione terroristica, tra cui: la propaganda, la raccolta di fondi, la comunicazione, l'organizzazione e il reclutamento. Per il terrorista infatti le modalità di sfruttamento del web sono infinite. Il gruppo può svolgere attività di tipo propagandistico, informativo, mobilitare i sostenitori e scovare nuovi adepti grazie anche alla possibilità di agire nell'anonimato.

Il fenomeno terroristico, infatti, così come l'intera società si è modificato con l'avvento delle tecnologie informatiche. Questo ha permesso ai terroristi di mutare le loro tradizionali attività, per esempio tramite l'uso dei social network si è riscontrata una maggiore immediatezza nelle comunicazioni e nel reclutamento. Tramite ciò si ampliano le opportunità dei terroristi ed intere attività che prima erano vincolate, in termini spaziali e temporali sono risultate più immediate e agevoli.

Difatti, fin dal 2010, si è incominciato ad osservare questa nuova modalità di terrorismo che si serve di Internet come strumento di azione. In ragione di ciò anche gli Stati e le Organizzazioni Internazionali governative hanno avvertito il bisogno di dare una risposta, per esempio l'Unione Europea nel 2013

[17] Europol, Eu terrorism situation and trend report, 2012,

ha stabilito una prima strategia di sicurezza per il cyberspazio[18] in cui un focus era dedicato ai cybercrimes e al cyberterrorismo.

Per questo nella corrente trattazione è stato ritenuto essenziale ribadire che quando si indaga sulla minaccia terroristica bisogna prestare attenzione all'uso di Internet. Sia nell'Agenda EU Controterrorismo sia nel Report di EUROPOL sulla "situazione terrorismo" è stata dedicata una sezione all'analisi della dilatazione dei contenuti terroristici tra le piattaforme online. Dalle suddette ricerche europee si può trarre la conclusione che "i terroristi usano la tecnologia digitale e Internet per i loro sforzi di propaganda e per le loro comunicazioni". Dalla precedente trattazione dell'attacco alla sinagoga in Germania si può inoltre estrapolare l'uso che gli attentatori fanno dei social media, per cui la diffusione delle ideologie radicali e del materiale di orientamento dei terroristi accelera attraverso l'uso della propaganda online. Questa esigenza di trasmissione in tempo reale delle loro azioni non rappresenta solo il bisogno di una postuma testimonianza, ma diventa parte integrante dell'attacco stesso.

Nel Rapporto di EUROPOL sulla situazione terrorismo del 2019 si è posta l'attenzione all'uso che i gruppi estremisti di destra fanno delle tecnologie e dei moderni sistemi di comunicazione. Si afferma che ad usare le nuove piattaforme di comunicazione, tra tutte le tipologie di gruppi terroristici, i più frequenti riscontrati sono gli estremisti di destra. Per esempio rispetto a gruppi jihadisti, nel 2019 è stato osservato, ad opera delle organizzazioni di destra, un maggior uso di piattaforme online tra cui siti web, social media, forum di discussione forum di discussione online e siti di pseudo-notizie, per diffondere la loro ideologia. La grande libertà d'azione che conferiscono questi canali è la ragione che spinge i terroristi ad usufruirne. In particolare è stato dedicato uno studio ai forum anonimi. Per partecipare a queste piattaforme non è necessaria alcuna registrazione. Data la garanzia di anonimato, questa tipologia di network diventa il luogo ideale per i potenziali terroristi per esprimere anonimamente intenzioni, ideologie e contenuti. Con un semplice post i terroristi portano a termine più attività: mentre esprimono le loro ragioni, commettono anche un'opera di diffusione e propaganda, incitano alla violenza ed ispirano nuove reclute.
Simili ai forum anonimi risultano essere anche i gruppi di comunicazione su app di messaggistica, nello specifico quei gruppi chiusi garantiti dalla crittografia.

Dopo aver esaminato l'estremismo di destra e le relative modalità di cyberterrorismo EUROPOL riporta

[18] EU Cyber Security strategy: *An open, safe and secure Cyberspace*; 2013.

anche delle considerazioni sui modi di agire online da parte dei gruppi di sinistra. Per questa tipologia di terroristi Internet si configura come uno strumento adatto ai fini di: sensibilizzazione, propaganda e reclutamento.

Le autorità preposte hanno sviluppato soluzioni innovative basate sulla tecnologia AI, ad esempio per identificare i contenuti terroristici online e fermarne la diffusione, per impedire la creazione di nuovi account di terroristi sui social media e per individuare i simboli di propaganda.

Dal 2016, per contrastare la diffusione dei contenuti terroristici online, è intervenuta anche l'Unione Europea. Nello specifico ci si riferisce al progetto TENSOR[19], avviato nel settembre 2016. TENSOR è stato avviato allo scopo di sviluppare una piattaforma di intelligence che aiutasse le forze dell'ordine a individuare rapidamente attività terroristiche e processi di radicalizzazione e reclutamento online. TENSOR si serve di una funzionalità automatica che permette la scoperta di contenuti terroristici e in seguito la loro: categorizzazione, analisi e filtraggio; è contemplata anche una intercettazione dei contenuti in tempo reale. L'ambito di applicazione di TENSOR nel cyberspazio è assai ampio, infatti spazia dalla parte di Web indicizzato- World Wide Web- fino al Deep e Dark Web.

A TENSOR è seguito un ulteriore progetto assai più recente: il progetto DANTE[20] del 2020. Anche quest'ultimo si configura come uno strumento di rilevazione e analisi di contenuti terroristici online e dell'attività di finanziamento del terrorismo. Anche DANTE si serve di un sistema autonomo ed integrato alla piattaforma per operazioni di *data mining* ed analisi.

Le attività dell'Unione, per il contrasto al fenomeno terroristico, di certo non terminano qui. Come riporta l'Agenda Controterrorismo EU di dicembre 2020 si è aperto il dialogo sulla possibilità di adottare una proposta di regolamento per la lotta contro la diffusione di contenuti terroristici online. Questo permetterebbe ad ogni Stato Membro applicante di garantire la rapida rimozione di tali contenuti e richiederebbe alle grandi aziende Web di essere più reattive nel prevenire l'abuso delle loro piattaforme. Tra le altre misure di cui l'Unione Europea intende servirsi nella sua strategia al controterrorismo, e nello specifico alla lotta alla profilazione di contenuti ideologici online, vi rientra una "*guida sulla moderazione dei contenuti"* elaborata dall' European Internet Forum[21]. Il Forum stesso rappresenta uno strumento istituito dall'Europa già nel 2015 allo scopo di riunire la Commissione EU,

[19] Per approfondimenti sul progetto TENSOR: https://cordis.europa.eu/article/id/415900-new-tools-help-law-enforcement-stop-online-terrorist-activity/it; https://tensor-project.eu/overview/aims-and-objectives/
[20] Per approfondimenti sul progetto DANTE https://www.h2020-dante.eu/it/
[21] Per approfondimenti su European Internet Forum https://www.internetforum.eu/

gli Stati membri, Europol, la rete di sensibilizzazione al problema della radicalizzazione (RAN) e le maggiori aziende Internet, per ridurre il proliferare della propaganda terroristica online e per mettere in atto un'opera di responsabilizzazione e sensibilizzazione. Secondo questa struttura, nel contrasto ai contenuti terroristici su Internet vi rientra anche l'incitamento all'odio online a sfondo razzista e xenofobo. Negli anni il Forum promuove riunioni periodiche per instaurare un maggiore coordinamento tra gli Stati Membri in tema di moderazione dei contenuti terroristici. In ultimo, l'impegno dell'Unione non si ferma all'interno dei propri confini, ma continua a livello mondiale. Difatti si impegna nel Global Internet Forum to Counter Terrorism[22] (GIFCT) anche con partner internazionali, le finalità del GIFCT sono principalmente tre:

1. Prevenire: cioè diffondere la consapevolezza tra i gestori delle piattaforme online che sono necessari strumenti per sviluppare politiche di contrasto all'attività terroristica e all'estremismo violento online;
2. Rispondere: tramite il coinvolgimento degli attori internazionali e di ogni altro soggetto interessato fornire una risposta concreta tentando di mitigare l'impatto di un attacco terroristico;
3. Apprendere: il Global Forum ha istituito anche un servizio di ricerca e delle aree prioritarie in cui concentrare i propri sforzi, tra cui per esempio analizzare il nesso tra comportamenti online e gli eventi reali.

Dopo aver analizzato l'Agenda EU Controterrorismo 2020 e i precedenti punti d'intervento dell'azione del GIFCT, si può affermare che la strategia sviluppata dalle istituzioni comunitarie ben si sposa con l'approccio internazionale di contrasto al terrorismo.

6. Protezione degli Spazi Pubblici

Negli ultimi due decenni la cooperazione europea sul controterrorismo ha portato notevoli miglioramenti e ha reso gli Stati Membri più capaci di assicurare la sicurezza dei loro cittadini. Ciò è stato reso possibile, soprattutto, attraverso la cooperazione giudiziaria, la cooperazione tra le forze di polizia e grazie alla fornitura di potenti strumenti utili a sottrarre ai terroristi i mezzi per poter effettuare attacchi sul suolo europeo. Nonostante i progressi, è necessario comunque incrementare lo sforzo così da contrastare la diffusione di ideologie estremiste e proteggere gli spazi pubblici, spesso bersaglio degli attacchi terroristici. Basti pensare ai recenti attentati avvenuti ai danni di nazioni

[22]Sito ufficiale *Global Internet Forum to Counter Terrorism* https://gifct.org/

europee, che per la maggior parte sono stati attuati in città metropolitane. Uno dei più significativi episodi che ci aiuta ad illustrare la minaccia alla pubblica sicurezza, è la strage di Nizza del 2016. In questo caso la maggior parte delle vittime da parte dell'attentatore non è stata fatta utilizzando armi convenzionali, ma servendosi di un comune camion e percorrendo per circa 2km la Promenade des Anglais durante le celebrazioni francesi per il 14 luglio. Data la consapevolezza che si è sviluppata tra i terroristi, di poter sfruttare le vicende quotidiane delle metropoli europee ai loro fini, la protezione degli spazi pubblici risulta essere uno dei punti fondamentali della nuova Agenda europea sul controterrorismo. Una maggiore protezione degli spazi pubblici, secondo l'Agenda europea, potrebbe essere facilitata dall'utilizzo di nuove tecnologie, tra le quali vengono indicate quelle di identificazione facciale capaci di individuare terroristi comparando la loro immagine facciale con quella contenuta nei database delle forze dell'ordine, e anche dall'utilizzo dell'Intelligenza Artificiale che potrebbe rivelarsi, anch'essa, molto utile nell'identificazione di nuove minacce.

Le nuove tecnologie, però, potrebbero anche rivelarsi portatrici di nuove insidie. I droni, ad esempio, potrebbero essere utilizzati in modo malevolo per bersagliare spazi pubblici, individui e infrastrutture critiche. Per via della rapida innovazione e del facile accesso ai droni la Commissione ha intenzione di affrontare questa minaccia rilasciando nel corso di quest'anno un manuale per la sicurezza della città (EU handbook for securing cities) e si è dichiarata pronta a finanziare progetti utili per lo sviluppo di nuove tecnologie all'interno dell'Agenda Urbana dell'Unione Europea. A partire dal gennaio 2021, inoltre, gli operatori di droni saranno obbligati a registrarsi presso le autorità nazionali. Per rendere più efficace questo sistema, esso dovrebbe essere integrato da un quadro normativo per l'U-space, il sistema europeo di gestione del traffico senza equipaggio, così da rendere più protette e sicure le operazioni coi droni. Oltre a questo saranno necessari ulteriori interventi che potrebbero includere "la condivisione di informazioni, orientamenti e buone pratiche e anche la sperimentazione su ampia scala di contromisure per i droni" (European Programme for counter-UAS systems testing).

La protezione degli spazi pubblici si va a inserire nel terzo pilastro dell'agenda europea sul controterrorismo, ossia il pilastro che riguarda, appunto, la protezione dei cittadini europei. Gli spazi pubblici risultano essere gli obiettivi privilegiati dei terroristi per i loro attacchi, a causa della loro vulnerabilità dovuta al loro facile accesso. Gli spazi pubblici dal più alto valore simbolico risultano essere i luoghi di culto, i quali sono frequentemente bersaglio di attacchi terroristici. La protezione di chiese, moschee e sinagoghe, così come altri siti religiosi sul suolo europeo, risulta essere un dovere fondamentale e un obiettivo da raggiungere, favorendo la cooperazione tra le diverse comunità di fedeli e le autorità nazionali al fine di migliorare il livello di sensibilizzazione in materia di sicurezza e contribuire all'attuazione delle buone pratiche e della formazione nei luoghi di culto.

Creare degli spazi pubblici più sicuri significa trovare un compromesso tra il rafforzamento della protezione fisica di tali luoghi e la libertà dei cittadini. Per poter raggiungere quest'obiettivo la Commissione aumenterà gli sforzi a livello europeo al fine di promuovere delle soluzioni **"Security-by-design"**, che metteranno la sicurezza negli spazi pubblici in primo piano sin dagli iniziali processi di pianificazione urbana. A tal proposito, la Commissione rilascerà un libro di architettura sul design urbano, che potrà servire come ispirazione per le autorità che decideranno di inserire elementi di sicurezza nella progettazione dei futuri spazi pubblici e anche nei progetti di rinnovamento degli spazi pubblici esistenti.

Il Forum europeo sulla protezione degli spazi pubblici ha messo insieme un vasto gruppo di persone con responsabilità nel settore della sicurezza degli spazi pubblici, come ad esempio autorità nazionali, ma anche operatori privati come i responsabili dei servizi di trasporto. La Commissione è impegnata nel rafforzamento di questo forum, il quale potrebbe essere fondamentale nella raccolta e nella divulgazione di conoscenze, nel supporto all' **"EU Pledge on Urban Security and Resilience"** e nel corretto utilizzo dei fondi comunitari per migliorare la protezione degli spazi pubblici. La Commissione potrebbe anche stabilire degli obblighi minimi da rispettare per i responsabili della sicurezza degli spazi pubblici così da rendere più chiaro cosa la Commissione si aspetta dagli operatori.

All'interno dell'European Forum for Urban Security[23] si sono sviluppati vari progetti di promozione della sicurezza all'interno degli spazi urbani, progetti sia a livello europeo che nazionale. Anche l'Italia ha aderito allo sviluppo di queste azioni, sia tramite collaborazioni per esempio all'interno del progetto PACTESUR[24], sia con politiche autonome come nel caso del piano per la città di Bologna e per la Regione Emilia Romagna, in cui ci si impegna a promuovere la legalità tramite il Testo Unico per la Promozione della Legalità e Valorizzazione della Cittadinanza e dell'Economia Responsabile.

Il progetto mira a responsabilizzare le città e gli attori locali nel campo della sicurezza degli spazi pubblici, soprattutto di fronte alle minacce terroristiche, ma anche contro altri rischi. Tramite PACTESUR l'Italia collabora con la Francia, difatti l'azione si sviluppa in tre specifiche città, quali: Nizza, Torino, Liège; allo scopo di attuare strategie comuni in materia di sicurezza urbana.

Il forum non è stata l'unica occasione in cui operatori pubblici e privati di spazi pubblici si sono riuniti. Il Centro comune di ricerca della Commissione, infatti, nell'ottobre 2020 ha organizzato una **Autumn School digitale dell'UE per la protezione degli spazi pubblici**, durante la quale sono stati esaminati diversi argomenti, "quali le modalità di protezione contro le esplosioni e i veicoli-ariete, l'attenuazione

[23] https://efus.eu/en/topics/risks-forms-of-crime/organised-crime-trafficking/efus/12079/

[24] Per approfondimenti sul progetto PACTESUR https://www.pactesur.eu/

delle minacce rappresentate da droni ostili in ambienti urbani, e l'uso di tecnologie di sorveglianza e rilevamento".

7. Riabilitazione e reintegrazione dei detenuti radicali

Nonostante la diminuzione generale del numero di attentati, la minaccia terroristica nell'Unione Europea rimane elevata, dal momento che la radicalizzazione potrebbe generare un'ampia polarizzazione e destabilizzare la coesione sociale. Sono gli Stati Membri a detenere la responsabilità nella lotta al terrorismo e alla radicalizzazione, ma la crescente dimensione transfrontaliera della minaccia richiede ulteriori passi in avanti per quanto riguarda la cooperazione e il coordinamento a livello europeo.

Combattere il terrorismo significa affrontare le cause più profonde del fenomeno. La polarizzazione della società, la discriminazione e altri fattori psicologici possono rendere le persone sempre più vulnerabili nei confronti del discorso radicale. Il contrasto della radicalizzazione va, quindi, di pari passo con la promozione della coesione sociale a ogni livello. Politiche non vincolanti come l'istruzione, la cultura e lo sport, potrebbero offrire un grande contributo nella prevenzione della radicalizzazione, offrendo opportunità per i giovani a rischio e favorendo, appunto, la coesione all'interno dell'Unione Europea.

Per favorire la coesione e riunire le comunità, la Commissione, il 24 novembre 2020, ha adottato un nuovo **piano d'azione sull'integrazione e l'inclusione**, che mira a offrire a tutti pari opportunità di godere dei propri diritti e di partecipare alla vita sociale e comunitaria, attraverso il rispetto dei valori comuni europei sanciti dai trattati e dalla Carte dei diritti fondamentali dell'Unione Europea.

In Europa sono state sviluppate diverse iniziative efficaci, quale ad esempio "**Le città dell'UE contro la radicalizzazione"**, un'iniziativa che si rivolge principalmente ai sindaci e ai loro consulenti che integra gli sforzi della rete UE di sensibilizzazione al problema della radicalizzazione, in particolare attraverso scambi politici tra città sulla prevenzione del fenomeno. Sembra, inoltre, ormai necessario prendere in considerazione azioni finalizzate a integrare le politiche, le iniziative e i fondi europei per contrastare la radicalizzazione.

È necessario che i processi di radicalizzazione vengano individuati il più presto possibile affinché le attività di disimpegno possano essere implementate in tempo. L'agenda europea sul controterrorismo, a tal proposito, propone il rafforzamento dell'azione europea in tre aree: **prigioni, riabilitazione e reintegrazione.**

Per prima cosa, andranno identificati gli approcci migliori per quanto riguarda la gestione e la valutazione del rischio dei detenuti radicali, così come andranno supportati i professionisti coinvolti

in questo campo (personale carcerario, cappellani, psicologi, ONG etc.). La Commissione, per esempio, crede che lunghi periodi di custodia cautelare possano incrementare il rischio di radicalizzazione. Per seconda cosa, prendendo spunto dall'esperienza del "**Radicalisation Awareness Network Rehabilitation Manual"**, la Commissione supporterà gli Stati Membri nella fornitura di un orientamento su misura per la riabilitazione e la reintegrazione dei detenuti radicali. Per terza cosa, verrà sviluppata una metodologia con standard e indicatori comuni al fine di valutare l'efficacia dei programmi di reintegrazione.

Portare a termine piani di riabilitazione e reintegrazione non è semplice e richiede un grande sforzo da parte di tutte le parti impegnate. Il manuale del *Radicalisation Awareness Network (RAN)* sulla "risposta ai combattenti terroristi stranieri di ritorno in patria e famiglie"[25] del 2017 descrive i diversi metodi e tipi di intervento utili per raggiungere lo scopo. La riabilitazione, per prima cosa, deve essere adattata all'autore del reato, prendendo in considerazione le sue esigenze e i suoi desideri, così da promuovere una buona cooperazione con il detenuto. I programmi di riabilitazione, inoltre, comprendono elementi di deradicalizzazione e disimpegno: con il primo termine si vuole indicare non solo un cambio nella mentalità del detenuto, ma soprattutto un cambiamento comportamentale e pratico; disimpegno, invece, è il termine utilizzato per questi cambiamenti[26].

Stando al manuale RAN sulla risposta ai rimpatriati, i piani di riabilitazione dei detenuti si rivelano efficaci se vengono eseguite determinate azioni: offrire interventi regolari a sostegno della riabilitazione attraverso attività ricreative aiuterà i detenuti a prepararsi al rilascio e al reinserimento nella società; lavorare sulla dimensione ideologica attraverso consulenze individuali, sessioni di dialogo di gruppo e attraverso l'incoraggiamento alla riflessione sulle proprie convinzioni; offrire sostegno religioso e spirituale aiuterà a ristabilire l'autostima e faciliterà il cambiamento comportamentale, allontanando i detenuti da ideologie religiose estremiste; ripristinare le relazioni positive con la famiglia e la rete sociale, evitando l'isolamento del detenuto; fornire sostegno psicologico e intervento per i traumi; offrire programmi di tutoraggio e mantenerli anche dopo il rilascio; lavorare con ex estremisti ed ex soldati, i quali, per via della loro esperienza, spesso godono di maggior rispetto agli occhi dei rimpatriati e saranno in grado di relazionarsi con loro.

In seguito ai programmi di riabilitazione intervengono i programmi di reintegrazione e reinserimento che mirano a prevenire comportamenti violenti e consentire l'inclusione e la partecipazione nella società. Affinché il reinserimento nella società proceda senza intoppi sarà necessario offrire

[25] Per approfondimenti: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/ran_br_a4_m10_it.pdf

[26] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/about-ran/ran-p-and-p/docs/ran_wrk_pp_pract_3rd-2018_20190606_it.pdf

sostegno al detenuto durante il periodo di libertà vigilata, ossia durante il periodo immediatamente successivo alla liberazione, offrire sostegno pratico, ossia la fornitura di un alloggio, ma anche la fornitura di una forma di sostegno finanziario attraverso il sistema di previdenza sociale. Sarà fondamentale, inoltre, offrire sostegno psicologico e ideologico riadoperando le stesse forme descritte per gli interventi in carcere, ma in un contesto comunitario. Non bisogna dimenticare, infine, il ruolo della famiglia che, nel caso in cui si dimostri una forza positiva di cambiamento può rivelarsi fondamentale nel processo di reinserimento.

I foreign fighters e i membri delle loro famiglie, inclusi quelli attualmente stanziati nei campi di detenzione nel Nord-Est della Siria, sollevano quindi sfide molto complesse, che richiederanno una forte cooperazione a ogni livello[27]. La Commissione, a tal proposito, sosterrà gli Stati Membri nella condivisione delle migliori pratiche in merito alle misure e ai meccanismi nazionali per gestire meglio la riabilitazione e il reinserimento dei combattenti terroristi stranieri rimpatriati (minori compresi), e aumenterà il supporto nei confronti degli operatori che operano in quest'area, facilitando la comprensione dei processi che portano alla radicalizzazione e all'estremismo violento, e migliorando l'approccio del settore giudiziario per quanto riguarda le condanne e le alternative alla detenzione. La Commissione sta anche lavorando a stretto contatto con gli Stati Membri e i paesi partner per garantire che le prove raccolte sui campi di battaglia siano condivise e utilizzate per l'identificazione. Nonostante il memorandum del 2020 sulle prove raccolte sul campo di battaglia di Eurojust dimostri che sia difficile ottenere certi dati, le prove raccolte possono contribuire a consegnare gli indagati alla giustizia.

La sfida costituita dai foreign fighters rende chiaramente visibile il legame che esiste tra sicurezza esterna e sicurezza interna. La cooperazione in materia di lotta al terrorismo e contrasto della radicalizzazione è fondamentale per la sicurezza all'interno del continente, ma è necessario anche sviluppare partenariati in materia di lotta al terrorismo con i paesi vicini. Il Consiglio Europeo ha infatti chiesto un ulteriore rafforzamento dell'impegno esterno dell'UE in materia di lotta al terrorismo, con particolare attenzione ai Balcani Occidentali, al Nord Africa, al Medio Oriente, alla regione del Sahel, al Corno d'Africa e all'Asia. Questo lavoro viene portato avanti attraverso i dialoghi ad alto livello sulla lotta al terrorismo e attraverso la rete di 17 esperti di antiterrorismo/sicurezza dispiegati presso le delegazioni dell'UE. Il punto di riferimento per le future cooperazioni in materia di antiterrorismo è il piano d'azione congiunto del 2018 sulla lotta al terrorismo per i Balcani occidentali, che comprende la gestione del rimpatrio dei foreign fighters e dei loro familiari e una forte integrazione nelle attività anti radicalizzazione. L'UE, inoltre, continuerà a promuovere la cooperazione multilaterale con i principali

[27] COM (2020) 795 final

organismi globali del settore, come le Nazioni Unite, la NATO, il Consiglio d'Europa, l'Interpol e l'OSCE. Anche il Consiglio Europeo, nel documento contenente le conclusioni derivanti dalle riunioni del 10 e 11 dicembre 2020, ha affermato l'importanza di evitare la radicalizzazione e di contrastare le ideologie connesse al terrorismo e estremismo violento, anche online, sottolineando l'importanza fondamentale della cooperazione giudiziaria e della condivisione di informazioni. Il Consiglio Europeo ha anche avanzato delle richieste, completamente in linea con l'agenda dell'UE per la lotta al terrorismo, riguardanti l'intensificazione della lotta contro i contenuti illegali online, l'adozione della proposta relativa al contrasto della diffusione di contenuti terroristici online, il contrasto di alcuni finanziamenti poco trasparenti indirizzati a organizzazioni civili e religiose nazionali, e un forte sostegno alle iniziative volte a comprendere meglio la diffusione delle ideologie estremiste.

8. Scambio informativo e cooperazione internazionale

Uno dei punti maggiormente ricorrenti nell'Agenda EU controterrorismo è l'importanza della condivisione di informazioni e della cooperazione internazionale tra Agenzie. La cooperazione europea è di stampo giuridico e giudiziaria, e si basa essenzialmente su reti di condivisione di informazioni, utilizzando gli strumenti delle banche dati. Accanto agli strumenti operativi ci sono le strutture deputate alla cooperazione, fra cui le principali sono: Eurojust ed Europol. Esse assicurano il coordinamento tra gli Stati Membri, lo scambio informativo, forniscono un quadro giuridico delle diverse legislazioni nazionali e forniscono delle risposte concrete in materia di sicurezza. Per questo la Commissione Europea si impegna a creare un dialogo tra gli operatori delle Agenzie investigative, utilizzando anche gli strumenti diplomatici dell'UE come il Servizio europeo per l'azione esterna- SEAE e l'European Union Intelligence and Situation Centre- EU INCEN.

Viene ribadita l'importanza di garantire la sicurezza nello spazio di Schengen. Si tratta dei controlli alle frontiere, che dal 1985 sono stati aboliti all'interno del territorio dell'Unione creando uno spazio di libera circolazione, ma rimane l'importanza dei controlli alle frontiere esterne. Per cercare di contrastare il terrorismo internazionale, cioè quello messo in atto da gruppi stranieri su un territorio diverso da quello di propria cittadinanza, che viene definito "Paese bersaglio"; si afferma la necessità di assicurare controlli maggiormente efficienti alle frontiere esterne. Queste vengono definite come il confine fra uno Stato Schengen e uno Stato non Schengen. La cooperazione è il valore alla base del funzionamento del sistema Schengen, inoltre questo spazio di sicurezza prevede anche delle regole precise di funzionamento, tra cui assicurare lo scambio informativo tramite il Sistema d'informazione Schengen (SIS) e al Sistema d'informazione Visti (VIS). Tramite questi reti di comunicazione si cerca di *"garantire la sicurezza dello spazio senza frontiere, gli Stati Schengen scambiano informazioni per far*

fronte alla criminalità transfrontaliera e al terrorismo".[28]

Accanto ai sistemi informativi di Schengen, vengono illustrati nuove istituzioni per garantire un sostegno rafforzato in materia di controterrorismo, nello specifico: Frontex ed EU-LISA. Sono entrambe delle Agenzie di cooperazione internazionale. la prima costituisce una guardia di frontiera e delle coste, mentre l'altra è l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia. Per garantire la sicurezza dei territori europei, è di fondamentale importanza che le autorità di contrasto possano individuare alle frontiere esterne sia i cittadini dell'UE che quelli extracomunitari sospettati di terrorismo. In questo senso Europol, Frontex ed eu-Lisa hanno il compito di sostenere ed assistere gli Stati membri.
La Commissione si augura che nel 2021 ci siano delle svolte in materia di cooperazione, nello specifico è stato annunciato che verrà rivisto il codice delle frontiere Schengen, verrà garantita la modernizzazione della gestione delle frontiere esterne a livello di ogni singolo Stato Membro e che dovrà essere assicurato il controllo sistematico di tutti i viaggiatori rispetto alle banche dati pertinenti alle frontiere esterne.
Nel frattempo, in attesa di questa innovazione normativa, restano cruciali i nuovi regolamenti del Sistema d'informazione Schengen (SIS), entrati in vigore nel dicembre 2018, che hanno introdotto una serie di misure per migliorare lo scambio di informazioni anche sui sospetti terroristi. In particolare, gli Stati membri dovrebbero urgentemente implementare la funzionalità di ricerca delle impronte digitali nel sistema automatizzato di identificazione delle impronte digitali (AFIS) del SIS ai loro funzionari, in particolare alle frontiere esterne.

È inoltre essenziale che le informazioni sui combattenti terroristi stranieri, fornite da paesi terzi fidati, siano inserite nel SIS. Insieme a queste previsioni, la Commissione Europea ha previsto un mandato Europol rafforzato e un emendamento al regolamento sull'istituzione, il funzionamento e l'uso del sistema d'informazione Schengen (SIS) che permetterebbe a Europol di creare segnalazioni dedicate nel SIS, in consultazione con gli Stati membri.

Ma la cooperazione in materia di controterrorismo non può risolversi soltanto tra gli Stati Membri. Difatti la minaccia terroristica non è solo di stampo internazionale, ma globale; per questo la collaborazione tra gli Stati europei e lo scambio informativo tra le Agenzie di sicurezza dell'Unione non basta. Gli strumenti di controterrorismo devono oltrepassare le frontiere esterne dell'Europa, per far

[28] *Un'Europa senza frontiere. Lo spazio Schengen*; Ufficio delle pubblicazioni- Commissione Europea. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/schengen_brochure/schengen_brochure_dr3111126_it.pdf

questo la Commissione Europea ha ribadito l'importanza di collaborare con Interpol. Interpol rappresenta l'organizzazione internazionale di polizia criminale ed un partner chiave nella lotta al terrorismo, per esempio grazie alla sua esperienza riguardo ai combattenti terroristi stranieri. Proprio per l'efficacia di Interpol nel raccogliere informazioni sul campo e nell'elaborare banche dati utili allo scambio informativo, alcuni organismi dell'UE si trovano di fronte alla necessità operativa di avere accesso alle banche dati di Interpol per svolgere i loro compiti. Per agevolare tale accesso e renderlo conforme con i requisiti della legislazione dell'UE, la Commissione ha dichiarato la propria disponibilità per elaborare un accordo di cooperazione tra l'UE e Interpol.

Conclusione

Il terrorismo, fenomeno umano e sociale, muta con il trasformarsi ed evolversi della società. I più evidenti adattamenti di questa forma di criminalità sono da notare nell'evoluzione dei propri strumenti, dei propri modi di colpire e nelle armi che utilizza.

Come si può evincere da questo lavoro, i sofisticati strumenti messi in campo dall'Unione Europea e dagli Stati Membri rendono evidente il fatto che il terrorismo sia, ancora oggi, un elemento di grande preoccupazione e una minaccia per le nostre società. Non bisogna, però, limitarsi unicamente al contrasto del terrorismo jihadista, il quale, sebbene risulti quello più pericoloso e più rilevante dal punto di vista mediatico, non è l'unico tipo di terrorismo da cui gli Stati devono difendersi. Il rapporto Europol, a tal proposito, analizza anche il terrorismo di tipo politico che, nonostante abbia perso l'impeto di qualche decennio fa, risulta essere presente e attivo in diversi Stati Membri dell'UE tra cui l'Italia, nazione in cui è stato rilevato il maggior numero di arresti nell'ambito dei movimenti eversivi di estrema sinistra.

Come evidenziato nella trattazione, un ruolo essenziale, ormai, nelle attività terroristiche è da assegnare alle nuove tecnologie e all'uso di Internet. Lo spazio cibernetico, che per definizione appare in-governato e deregolamentato, fa si che anche i fenomeni criminali, quali quello terroristico, trovino meno limiti e freni. Difatti, sarà sempre più complicato, per le forze dell'ordine, per le istituzioni e le Agenzie di sicurezza, cercare di arginare la minaccia terroristica ibrida (i.e. le forme tradizionale e comuni di terrorismo che si mescolano con la criminalità online) con strumenti tradizionali.

Il contrasto al terrorismo può risultare efficace non solo attraverso l'uso delle armi e l'invio di "boots on the ground" nei Paesi d'addestramento e d'origine delle organizzazioni terroristiche. È necessario, infatti, agire anche nel campo sociale e promuovere attività di deradicalizzazione, riabilitazione e reintegrazione a favore dei soggetti più pericolosi e dei foreign fighters di ritorno dai campi di battaglia mediorientali e balcanici. Le attività di deradicalizzazione, a tal riguardo, sono fondamentali per evitare che i cittadini europei abbraccino tali ideologie estremiste e possano espandere la propria influenza in quelle zone più arretrate del continente dove vivono soggetti vulnerabili e quindi influenzabili da queste narrazioni estremiste.

Per questo è essenziale prevenire e contenere la diffusione delle ideologie terroristiche all'origine. L'Agenda EU per il contrasto al terrorismo si configura con un primo strumento tramite cui intervenire, ma accanto alle linee guida europee dovranno instaurarsi anche le direttive nazionali. L'approccio di cooperazione internazionale appare un decisivo punto cardine su cui basarsi, per far si che gli Stati,

sia europei che Terzi, intervengano in maniera congiunta contro un fenomeno transazionale che supera ogni forma di frontiera. Rispetto alle frontiere esterne dell'Unione Europea, si ritiene che in questo campo si dovranno ancora svolgere enormi sforzi, per cercare di arginare il fenomeno terroristico internazionale che contamina anche le principali rotte migratorie (irregolari).

Il contrasto al terrorismo, infine, passa anche dal controllo e dalla recisione delle linee di finanziamento delle attività terroristiche, le quali, attraverso il sistema dell'*hawala*, risultano essere difficilmente rintracciabili. L'Unione Europea e i suoi Stati Membri, perciò, dovranno far in modo di coordinare nel miglior modo possibile le attività di controllo e vigilanza attraverso la creazione di nuove istituzioni ad hoc e la cooperazione interstatale, la quale è alla base del processo di integrazione europeo.

In ultimo, è da tenere a mente, che il decremento degli attacchi compiuti sul territorio europeo dal 2018 al 2020, non è da considerare come la sconfitta del terrorismo; al contrario, questo deve ritenersi un campanello di allarme, grazie al quale continuare a studiare ed analizzare le emergenti e moderne forme di terrorismo.

La vittoria nella battaglia contro il terrorismo è ancora lontana, le organizzazioni terroristiche, nonostante le difficoltà, sembrano essere un grande esempio di resilienza e resistenza, ma questo non deve in nessun modo scoraggiare i Paesi Occidentali e portare a un allentamento della presa. È ormai chiaro agli occhi di tutti che le soluzioni militari non riescano a portare a una sconfitta definitiva del fenomeno, ma, anzi, spesso ne alimentano la ferocia e la pericolosità, quindi, sembrerebbe preferibile, dopo due decenni di lotte armate e vite spezzate, iniziare ad agire in maniera più efficace sull'inclusione delle comunità e degli individui più a rischio nelle nostre società.

Glossario:

- Controterrorismo: *Attività volta a prevenire, rilevare, contenere e contrastare le condotte di natura terroristica, ivi incluse quelle di carattere prodromico e/o strumentale. Comprende le iniziative tese a monitorare i contesti eversivo-terroristici, disarticolare gruppi e cellule, inibire le pianificazioni offensive di sodalizi e singoli individui e contrastarne le attività di propaganda, indottrinamento e reclutamento.*[29]

- Antiterrorismo: *Per contrastare il fenomeno terroristico viene messa in campo una complessa attività informativa di prevenzione, volta a prevenire le minacce alle istituzioni democratiche*. [30]

- Estremismo violento: *le manifestazioni - specialmente quelle attinenti alla sfera politica - più illiberali del massimalismo, del radicalismo e dell'intransigenza, spesso accompagnate dall'eversione e dalla violenza, sia quest'ultima palese o clandestina.* [31]

- Radicalizzazione: *il processo attraverso il quale si adotta un sistema di valori estremista, inclusa la volontà di usare, supportare o facilitare la violenza come metodo per il cambiamento sociale*[32]

- Terrorismo Internazionale: *Atti violenti e criminali commessi da individui e/o gruppi che sono ispirati da, o associati a, organizzazioni terroristiche straniere designate o nazioni (sponsorizzate dallo stato).*[33]

- Terrorismo Domestico: *Atti violenti e criminali commessi da individui e/o gruppi per promuovere obiettivi ideologici derivanti da influenze interne, come quelli di natura politica, religiosa, sociale, razziale o ambientale*.

[29] Glossario D'Intelligence- *IL LINGUAGGIO DEGLI ORGANISMI INFORMATIVI*, PRESIDENZA DEL CONSIGLIO DEI MINISTRI, Sistema di informazione per la sicurezza della Repubblica- 2013.
[30] https://www.interno.gov.it/it/temi/sicurezza/antiterrorismo
[31] http://gnosis.aisi.gov.it/sito/Rivista23.nsf/servnavig/7
[32] C.E. ALLEN, Threat of Islamic Radicalization to the Homeland, hearing allo United States Senate Committee on Homeland Security and Government Affairs, March 14, 2007,
[33] https://www.fbi.gov/investigate/terrorism

Bibliografia:

FATF Report: Emerging Terrorist Financing Risk – October 2015

FATF: COVID-19-Related Money Laundering and Terrorist Financing. Risks and Policy Responses – May 2020

Documento di lavoro della RAN, terza edizione 2018, "Approcci alla lotta alla radicalizzazione e al trattamento degli estremisti e dei terroristi violenti autori del reato in carcere e in regime di libertà vigilata".

Manuale RAN, *Risposta ai combattenti terroristi stranieri di ritorno in patria e famiglie*, giugno 2017

"Relazione sulla politica dell'informazione per la sicurezza" del comparto intelligence (Dis, Aise e Aisi) , 2020

Aragona V., *La rilevanza delle forme di partecipazione e di supporto al terrorismo,* in "Diritto penale contemporaneo", gennaio 2017

Commissione Europea, *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond,* dicembre 2020

Commissione Europea, *Comunicazione della Commissione relativa a un piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo,* maggio 2020

Commissione Europea, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regione sulla strategia dell'UE per l'Unione della sicurezza,* luglio 2020

Commissione Europea, *Prima relazione sui progressi compiuti nella strategia dell'UE per l'unione della sicurezza,* dicembre 2020

Europol, *European Union Terrorism and Trend report 2020*

TACTP o perossido di acetone: quali criticità per l'intervento operativo degli specialisti; Scaini Stefano / Auddino Lorenzo / Canfarini Federico; Analytica for intelligence and security studies- Paper Crisis Management; 2020.

LE ARMI DI DISTRUZIONE DI MASSA; Stefano Felician; CASD; Ministero della Difesa.

EU Cyber Security strategy: *An open, safe and secure Cyberspace*. 2013.

Glossario D'Intelligence- *IL LINGUAGGIO DEGLI ORGANISMI INFORMATIVI*, PRESIDENZA DEL CONSIGLIO DEI MINISTRI, Sistema di informazione per la sicurezza della Repubblica- 2013.

C.E. ALLEN, Threat of Islamic Radicalization to the Homeland, hearing allo United States Senate Committee on Homeland Security and Government Affairs, March 14, 2007.

Sitografia:

https://www.riskcompliance.it/news/hawala-un-sistema-illegale-per-il-finanziamento-al-terrorismo/

https://www.consilium.europa.eu/it/policies/fight-against-terrorism/fight-against-terrorist-financing/

https://www.anarcopedia.org/index.php/Federazione_Anarchica_Informale

http://www.robertobartali.it/cap05.htm

https://ctc.usma.edu/a-profile-of-the-informal-anarchist-federation-in-italy/

https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology/

https://www.agendadigitale.eu/sicurezza/droni-civili-a-scopo-offensivo-problemi-e-soluzioni/

TENSOR: https://cordis.europa.eu/article/id/415900-new-tools-help-law-enforcement-stop-online-terrorist-activity/it;

https://tensor-project.eu/overview/aims-and-objectives/

DANTE https://www.h2020-dante.eu/it/

https://www.fbi.gov/investigate/terrorism

https://www.interno.gov.it/it/temi/sicurezza/antiterrorismo

http://gnosis.aisi.gov.it/sito/Rivista23.nsf/servnavig/7