Analytical Dossier 08/2023
ISSN 2704-6419

RADICALIZZAZIONE ISLAMICA ONLINE

IL BILANCIAMENTO TRA SICUREZZA PUBBLICA E PRIVACY

Giorgia Pagliuca

International Institute for Global Analyses

Vision & Global Trends. International Institute for Global Analyses
Piazza dei Navigatori 22, 00147 – Rome (Italy)

First Edition: September 2023

Analytical Dossier 08/2023 - ISSN 2704-6419

www.vision-gt.eu
info@vision-gt.eu

Analytical Dossier 08/2023
ISSN 2704-6419

RADICALIZZAZIONE ISLAMICA ONLINE

IL BILANCIAMENTO TRA SICUREZZA PUBBLICA E PRIVACY

Giorgia Pagliuca

Vision & Global Trends - International Institute for Global Analyses

Analytical Dossier 08/2023
ISSN 2704-6419

INDICE

CAPITOLO 1

ABSTRACT

Il Web ha mutato i rapporti sociali e il modo di interagire, annullando i limiti dello spazio e del tempo.

Vivere senza internet è diventato pressoché impossibile, siamo costantemente connessi e reperibili, pronti a pubblicare qualsiasi cambiamento sui social network.

Lo smartphone, sul quale riceviamo un'enorme quantità di notifiche, è sempre al nostro fianco ed è pronto a raccogliere i nostri dati, utilizzati da terzi con le finalità più disparate.

Online è stata costruita una vera e propria comunità senza confini che permette a chiunque di condividere i propri pensieri e consente a simili di incontrarsi, anche se solo virtualmente.

Lo scopo di questa tesi è illustrare in che misura la rivoluzione digitale abbia modificato il modo in cui i terroristi islamici convincono i loro adepti a partire per il jihad.

Inoltre, è stato analizzato come questi si servano dei principali strumenti di comunicazione online al fine di diffondere il proprio messaggio, oltre che per glorificare i martiri o rivendicare attentati.

Attraverso report e indagini svolte da fonti come *Tech Against Terrorism, l'UE e RAND,* sono stati esaminati siti web*,* in ambiente *surface* e *dark,* piattaforme di *e-gaming,* social media e app di messaggistica al fine di analizzare in che modo il *cyber* jihad abbia creato un nuovo tipo di terrore.

Quel che è emerso è che ognuna delle piattaforme sopracitate è "invasa" da proselitismo, per diversi scopi e in differenti forme.

Una delle conseguenze della scelta dell'ISIS di spostare il califfato dalla Siria al mondo digitale è stata il maggiore controllo che i governi hanno deciso di esercitare sui loro cittadini, a scapito degli aspetti di privatezza delle comunicazioni personali.

Dinamiche di questo tipo sottolineano l'importanza di trovare un bilanciamento tra privacy e sicurezza pubblica.

CAPITOLO 2

Internet ha apportato enormi cambiamenti alla vita delle persone: da strumento esclusivo ed elitario per l'immagazzinamento di dati tecnici e scientifici, è diventato un mezzo di comunicazione e di informazione di massa accessibile a tutti.

Il Web ha decisamente cambiato le interazioni all'interno della società.

Ci ha permesso di costruire una realtà vita virtuale parallela che ci ha resi più coraggiosi e ci ha invogliati ad esprimere le nostre idee, opinioni e gusti; ma la rete ha anche un lato oscuro: cyberbullismo, adescamento e dipendenza da internet.

Attualmente, vi è un fenomeno in forte crescita che è necessario portare all'attenzione di tutti; si tratta di una questione meno nota, ma sommamente pericolosa: la radicalizzazione.

La rete non solo ha trasformato la comunicazione e semplificato l'interazione tra persone che condividono linee di pensiero e ideologie, ma ha anche avuto importanti ripercussioni sull'organizzazione e sul funzionamento della società e, poiché estremisti e terroristi ne sono parte integrante, è opinione diffusa che Internet svolga un ruolo particolare come strumento di radicalizzazione.

Se consideriamo vera la citazione "la società in rete è una società ipersociale, non una società di isolamento"[1] capiamo quanto diventi ogni giorno più importante prestare attenzione ad alcuni termini quali: terrorismo, radicalizzazione e radicalizzazione online.

La definizione del concetto di terrorismo genera ancora molte discussioni. Il termine venne utilizzato per la prima volta alla fine del Settecento quando Sir Edmund Burke, a commento di quanto visto in Francia, disse: "Si aggiravano per le strade migliaia di cani indiavolati chiamati *terroristi*".

Tuttavia, non esiste ancora una definizione accettata universalmente del concetto di terrorismo.

La NATO propone la seguente definizione:

> "L'uso o la minaccia di uso di comportamenti illegali o violenti contro individui o proprietà nel tentativo di condizionare o intimidire governi o società per raggiungere obiettivi politici, religiosi o ideologici."

La CIA propone la seguente definizione:

[1] Come sostenuto da Castells e Cardoso (2005)

> "Il termine terrorismo indica una violenza premeditata, motivata politicamente, condotta contro obiettivi civili da gruppi subnazionali o agenti clandestini".[2]

L'enciclopedia Treccani propone:

"L'uso di violenza illegittima, finalizzata a incutere terrore nei membri di una collettività orga nizzata e a destabilizzarne o restaurarne l'ordine, mediante azioni quali attentati, rapimenti, dirottamenti di aerei e simili."

Dal 2001 il terrorismo ha assunto un carattere internazionale: sempre più cittadini europei scelgono la via della radicalizzazione sfruttando, grazie al progresso tecnologico, anche il potere dei social network.

La radicalizzazione è definita dalla comunità europea come "il fenomeno che vede persone abbracciare opinioni, vedute e idee che potrebbero portare ad atti terroristici". Da luglio del 2017 è stata istituita la Commissione speciale sul terrorismo dell'UE che non si occupa esclusivamente dei controlli alle frontiere, del contrasto dei *foreign fighters* o del taglio delle risorse finanziare ai terroristi, ma dal 2020 ha anche lavorato in ottica di un incremento della sicurezza informatica.

Considerando il fatto che nel mondo sono 4,54 miliardi le persone con accesso ad Internet[3] e, di questi, circa 3,4 miliardi di utenti usano quotidianamente i social network, è facile comprendere come le idee viaggino più rapidamente su Internet di quanto lo facciano nel mondo fisico ed è altrettanto intuibile il motivo per cui i gruppi jihadisti abbiano scelto di servirsi di queste piattaforme.

Dunque, ci si sta interfacciando con un tipo innovativo di radicalizzazione, quella che avviene attraverso "un processo nel quale gli individui tramite le loro interazioni online e l'esposizione a vari tipi di contesto Internet, arrivano a considerare la violenza come un metodo legittimo per risolvere i conflitti sociali e politici"[4].

La rivoluzione dell'informazione iniziata negli anni '90 ha assunto un significato sociale crescente: oggi siamo travolti da informazioni che provengo da e-mail, social media o messaggi, in qualsiasi momento della giornata.

---

[2] Con riferimento al sito web della Central Intelligence Agency (CIA)

[3] Dati del rapporto "We Are Social 2020"

[4] (Bermingham 2009)

Tuttavia, questa rivoluzione digitale offre ai terroristi e agli estremisti le stesse opportunità e capacità che propone al resto della comunità cibernetica: comunicare, collaborare e convincere.

Per comprendere l'importanza di Internet per la radicalizzazione è sufficiente porsi le domande giuste: che ruolo gioca Internet rispetto all'apparente fenomeno della radicalizzazione online? È solo una fonte di ispirazione o accelera il processo di radicalizzazione? Questa può tradursi anche in azione?

Il Web ha garantito sicurezza, accessibilità e riservatezza agli eversivi che hanno spostato molte delle loro attività dagli spazi pubblici (si pensi alle moschee nel caso dei gruppi islamici) alle proprie abitazioni, transizione che permette loro, direttamente dal computer portatile, smartphone o tablet, di raggiungere il resto del mondo.

Questo cambiamento nel comportamento dei terroristi riflette l'impronta digitale in espansione nella società, in cui le attività quotidiane si spostano senza soluzione di continuità tra i domini online e offline.

“Internet ha trasformato la misura in cui le organizzazioni terroristiche e i loro simpatizzanti possono radicalizzare le persone in questo paese e all'estero.

Consente a una gamma più vasta di organizzazioni e individui di raggiungere un pubblico molto più esteso con una serie più ampia e dinamica di messaggi e narrazioni. Incoraggia l'interazione e facilita il reclutamento. Anche il modo in cui le persone usano Internet sembra favorire questi processi”.[5]

Tutte queste piattaforme non rappresentano una minaccia in sé per sé, ma la possibilità di avviare chat *room* criptate consente lo svolgimento di attività criminali o terroristiche.

A tal proposito è degno di nota l’utilizzo che i terroristi fanno del *gaming*.

Fino al 2020 tale ambito non rientrava tra gli sforzi dell’UE concernenti l’attività di antiterrorismo, ma queste piattaforme, non supervisionate a sufficienza, sono a rischio di abusi da parte degli eversivi, soprattutto jihadisti.

Le minacce poste dall’uso del *gaming* da parte degli estremisti sono varie: propagazione, radicalizzazione e reclutamento, comunicazione, addestramento al combattimento e riciclaggio[6].

[5] Prevant strategy- UK Home Office, 2011.

[6] Online gaming in the context of the fight against terrorism. Bruxelles, 6 luglio 2020.

Più fattori concorrono a rendere le piattaforme di gioco luoghi particolarmente attraenti per il reclutamento e la diffusione di propaganda violenta: un vasto pubblico di videogiocatori (cifra che corrisponde al 51% dei giovani tra i 15 e i 24) attratto principalmente dagli “sparatutto" e la disponibilità di servizi di interazione con gli altri all’interno dei giochi, attraverso i quali i terroristi possono sfruttare la vulnerabilità degli utenti, anche tramite avatar, che garantiscono un buon livello di riservatezza ..

La comunicazione in queste piattaforme è esteta e consente lo scambio di messaggi digitali crittografati.

In aggiunta, il frequente riferimento alle armi e alla violenza, come parte integrante di questi giochi, rende più difficile l'identificazione automatica di profili che possono rivelarsi una minaccia per la società.

In conclusione, dato che la comunicazione di gioco non viene sufficientemente presa in considerazione dalle autorità, questa è stata spesso trascurata a favore della sorveglianza di sistemi di telecomunicazione più convenzionali.

A livello di addestramento al combattimento, l’*e-gaming* aiuta a desensibilizzare i giovani alla violenza e fornisce loro competenze quali pianificazione della missione, equipaggiamento e tattiche. L’ultima minaccia affrontata dalla delegazione europea a Bruxelles il 6 luglio 2020 riguarda il riciclaggio di denaro: l’*e-gaming* ha dato vita a un’economia virtuale che permette di scambiare valuta reale al di fuori del videogame.

Questo sistema di scambio di denaro nel *gaming* non ha ricevuto la stessa attenzione e supervisione del *gambling*[7], ad esempio, e viene costantemente sfruttato da chi ha bisogno di riciclare denaro o finanziare organizzazioni in modo rapido, semplice e invisibile.

La rete, quindi, aumenta le opportunità di radicalizzazione perché rappresenta un mezzo attraverso il quale si può entrare in contatto con materiale coerente con le proprie ideologie e con persone che la pensano allo stesso modo senza dover uscire di casa.

[7] Gioco d’azzardo

2.1 RADICALIZZAZIONE ONLINE

"Ai fini della presente legge per radicalizzazione si intende il fenomeno delle persone che, anche se non sussiste alcuno stabile rapporto con gruppi terroristici, abbracciano ideologie di matrice jihadista, ispirate all'uso della violenza e del terrorismo, anche tramite l'uso del Web e dei social network"[8].

Le dimensioni del fenomeno di radicalizzazione nel nostro Paese sono inferiori rispetto agli altri e possiamo rilevare due principali ragioni alla base di tale affermazione:

- Minor tempo intercorso dall'inizio dei flussi migratori[9]: l'Italia è un caso particolare tra gli Stati dell'Europa Occidentale; non presenta ancora terze generazioni di migranti, essendo diventata un paese di immigrazione in anni relativamente recenti, per cui le comunità islamiche si sono formate soprattutto a partire dai flussi iniziati negli anni Novanta. Le motivazioni vanno ricercate nel fatto che la maggior parte delle migrazioni di comunità musulmane verso l'Europa è avvenuta dopo la Seconda guerra mondiale. I principali flussi coinvolgevano lavoratori delle ex colonie europee: la Germania ne ha ricevuto un gran numero dalla Turchia; la Gran Bretagna ha portato lavoratori dall'India, dal Pakistan e dal Bangladesh; la Francia dipendeva da immigrati algerini e marocchini; la Spagna faceva affidamento sui marocchini.

- L'Italia ha già fronteggiato il terrorismo: tra il 1960 e il 1980 il Bel Paese è stato costellato da una moltitudine di attacchi terroristici caratterizzati da un'estremizzazione della dialettica politica. Tale periodo è passato alla storia con il nome di "anni di piombo". In ragione dell'emergenza terroristica sono stati varati atti legislativi con la finalità di contrastare la violenza e sono stati creati corpi speciali delle forze dell'ordine come il GIS[10] e il NOCS[11].

[8] proposta di legge Dambruoso-ManciullI Art 1 comma 2

[9] cittadini stranieri musulmani residenti in Italia al 1° gennaio 2022 in 1,5 milioni, il 29,5% del totale dei cittadini stranieri, in aumento rispetto allo scorso anno

[10] Gruppo intervento speciale dei carabinieri

[11] Nucleo operativo centrale di sicurezza della polizia

Tra gli ambienti più idonei alla radicalizzazione troviamo gli istituti penitenziari[12] a causa della privazione della libertà, della pressione del gruppo e dell'isolamento dalla società, ma anche per via dell'emarginazione sociale e della violenza psicologica e fisica.

Tuttavia, un altro luogo nevralgico, in costante crescita, è il Web.

Verrebbe da chiedersi cosa abbiano in comune la rete e il carcere e la risposta la si può trovare nei processi di socializzazione e nella rabbia nei confronti di una società da cui questi soggetti si isolano.

Tuttavia, i luoghi sopracitati, il Web e il carcere, dovrebbero avere una funzione educativa (o rieducativa, nel caso del carcere), ma spesso così non è.

La differenza tra i due ambienti è evidente: l'istituto penitenziario è uno spazio stretto e limitato, quindi facile da controllare; il Web, proprio per il suo essere *World Wide*, ci offre una vastità di informazioni senza limite geografico o temporale.

È interessante notare la particolarità della radicalizzazione online in quanto essa avviene tramite un metodo chiamato *self radicalization:* l'auto-radicalizzazione.

Questa ha luogo quando un individuo inizia ad avvicinarsi a un'ideologia senza essere entrato in contatto con un gruppo eversivo.

L'ISIS[13] ha creato un vero e proprio marchio online: è possibile trovare siti destinati al merchandising, social media dedicati alla propaganda su cui è possibile chattare con predicatori e, utilizzando le *keywords* giuste, è possibile imparare a costruire un giubbotto esplosivo su YouTube.

Prendiamo ad esempio il caso di Maria Giulia Sergio, la ventenne campana studentessa di Biotecnologie presso l'Università di Milano.

Maria si è convertita all'Islam grazie ai video del predicatore texano Yusuf Estes, dopo aver preso contatti online con Bushra Haik[14], Maria, ora Fatima, ha deciso di compiere la sua هجـــرة (Hijra)[15] verso la Siria. Dal 2014 ha scelto spontaneamente di ampliare le file dei *foreign fighters*.

---

[12] Relazione del Ministero sull'amministrazione della giustizia - anno 2017- Capitolo 4,3.

[13] Stato islamico di Siria ed Iraq

[14] Trentacinquenne di origine siriana, nata a Bologna; considerata la maestra del jihad, è stato emesso nei suoi confronti un mandato di cattura internazionale nel 2015.

[15] dall'arabo: emigrazione

La tecnologia è ormai accessibile a tutti ed è quindi al servizio di "buoni e cattivi" senza distinzioni.

A partire dal G7, tenutosi nel 2015, sono state avviate un'enorme quantità di iniziative volte a rimuovere i contenuti terroristici da internet e ad impedirne la diffusione, a migliorare le nostre conoscenze di base attraverso ricerca e sviluppo e a pianificare nuove forme di cooperazione tra gli stati. Tuttavia, i terroristi sono stati resilienti e hanno continuato ad adattare i loro metodi affinché i contenuti trovassero il modo di rimanere disponibili online.

2.2 UTILIZZO CHE FANNO I TERRORISTI DI INTERNET

È innegabile che i social network abbiano alimentato le rivolte popolari del 2011 nel Nord Africa. Hanno apportato contributi positivi infondendo nella popolazione la necessità di democrazia e libertà. Non solo, hanno anche permesso la diffusione della comunicazione e di prendere parte al malcontento della popolazione.

Purtroppo, quella delle primavere arabe e dei social network è stata una storia avvincente con un finale drammatico in quanto nell'area MENA[16], oggi più di 12 anni fa, la democrazia ha perso e i social media sono invasi da proselitismo digitale utilizzato dai jihadisti.

La scienza della quale si servono i terroristi è la captologia[17], essa rappresenta la capacità di convincere l'interlocutore attraverso l'uso di tecnologie.

B.J. Fogg, professore di scienze comportamentali presso la Stanford University, ha elencato i mezzi attraverso i quali la tecnologia, a differenza dell'uomo, può influenzare il comportamento degli individui, tra gli altri troviamo: persistenza (si pensi ad esempio ad ogni volta che ci viene chiesto di registrarsi ad un sito), anonimato, big data, modalità differenti (es. video, audio, messaggi), rapida trasmissione di messaggi e, infine, ubiquità[18].

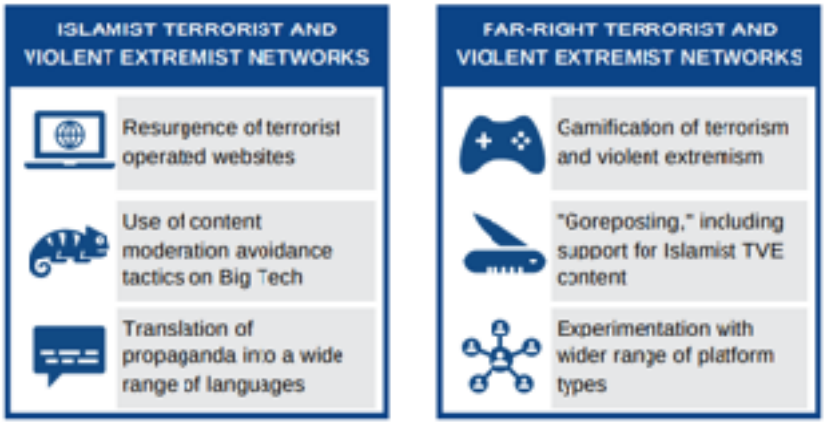
Alcune informazioni importanti sul reale utilizzo che i terroristi fanno di internet ci sono state offerte dal rapporto del 20 gennaio 2023 di Tech Against Terrorism.

Il rapporto esamina i luoghi dove i terroristi agiscono e le loro modalità di svolgimento:

[16] Middle East and North Africa

[17] termine coniato nel 1996 da J.B.Fogg

[18] Persuasive Technology: Using Computers to Change What We Think and Do di B.J.Fogg



- Websites. I terroristi utilizzano tanto il surface web quanto i siti "onion".

  Tra l'enorme quantità di obiettivi troviamo: conservazione di contenuti ufficiali, finanziamenti e comunicazioni.
- Big Tech. YouTube, Facebook e Telegram rappresentano solo tre tra le molteplici piattaforme che i terroristi utilizzano per condividere informazioni e file, fare propaganda e vendere prodotti online; il report evidenzia anche il modo in cui i terroristi sfruttino lingue differenti dall'inglese e l'arabo affinché i contenuti permangano per tempi più lunghi.

  Queste piattaforme permettono di raggiungere un pubblico vasto ad un costo minimo e non vengono solo utilizzate per diffondere materiale e reclutare adepti ma anche per encomiare gli attentati.
- Gaming. Molti giochi sono utilizzati per simulare attacchi reali e diversi attacchi sono organizzati come giochi, si pensi a Christchurch nel 2019[19]: l'attacco è stato filmato con una telecamera montata sul casco per emulare i giochi di genere "sparatutto" in prima persona.

[19] https://ctc.westpoint.edu/christchurch-attacks-livestream-terror-viral-video-age/

- Dark web. È utilizzato meno di quel che si pensa dai terroristi, che prediligono app di messaggistica crittografata, ma è probabile che queste reti decentralizzate saranno utilizzate più frequentemente nel futuro in quanto la lotta al terrorismo online si sta evolvendo.

Dal 2014, anno della proclamazione della nascita del califfato di Abu Bakr al-Baghdadi, l'IS ha incrementato la propria presenza sul Web e, di conseguenza, l'UE ha avviato una serie di iniziative che comprendono[20]: (a) prevenzione degli attentati e della radicalizzazione, (b) rimozione dei contenuti entro un'ora dai social media, (c) digitalizzazione della cooperazione giudiziaria e infine (d) ha avviato una lotta al riciclaggio e al finanziamento del terrorismo.
L'ISIS ha risposto alla censura spostando le proprie comunicazioni su piattaforme con messaggistica crittografata.

2.3 CRITTOGRAFIA E2E

La crescente preoccupazione degli utenti per la loro privacy online ha spinto diverse aziende ad offrire servizi di cifratura per le loro comunicazioni.
Le app di messaggistica sono utilizzate dall'87% della popolazione e la maggior parte di queste offre servizio di End-to-End (E2E) come default o opzionale.
"La crittografia end-to-end di WhatsApp viene impiegata quando avvii una chat con qualcuno tramite WhatsApp Messenger.
La crittografia end-to-end garantisce che solo tu e la persona con cui stai comunicando, e nessun altro, nemmeno WhatsApp, possiate leggere o ascoltare i contenuti inviati.
Con la crittografia end-to-end, i tuoi messaggi sono protetti con un lucchetto, e solo tu e il tuo destinatario avete la chiave speciale necessaria per sbloccarli e leggerli. Tutto questo avviene

[20] https://www.consilium.europa.eu/it/policies/fight-against-terrorism/

automaticamente: non c'è bisogno di attivare alcuna impostazione o creare speciali chat segrete per proteggere i messaggi[21]".

La crittografia è la scienza delle scritture segrete, un insieme di tecniche matematiche che rendono inintelligibile una determinata informazione a chi non è a conoscenza di una chiave per decifrarlo.

Concetto fondamentale della crittografia moderna è un sistema composto da due parti separate e indipendenti: (a) cifrario, il metodo che uso per codificare o algoritmo e (b) chiave, informazione segreta, diversa in ogni istanza[22].

La crittografia contemporanea può essere simmetrica ovvero la stessa chiave viene utilizzata per crittografare e decrittografare da entrambi gli interlocutori parte della conversazione, e asimmetrica, nella quale entrambe le parti dispongono di due chiavi: una pubblica e una privata, in cui la prima è disponibile per chiunque, mentre la seconda è personale, ad uso esclusivo del mittente.

Garantire la riservatezza delle comunicazioni è l'obiettivo di queste piattaforme di messaggistica, ma, oggi più che mai, è fondamentale trovare un equilibrio con la prevenzione.

Si pensi, ad esempio, a Telegram, l'app ideata da Pavel Durov, che, oltre ad offrire un servizio opzionale di crittografia e2e, consente di impostare un timer di autodistruzione che permette la cancellazione di messaggi e media subito dopo essere stati visualizzati.

Per via della privacy offerta da Telegram, l'applicazione è diventata popolare come mezzo di comunicazione tra i membri dell'IS e i suoi simpatizzanti.

Telegram nasce nel 2013, nel 2016 raggiunge 100 milioni di utenti attivi ed è disponibile per i principali sistemi operativi. Offre la possibilità di aprire dei canali che permettono l'invio di file in contemporanea a tutti gli utenti iscritti ad essi.

Daesh[23] ha aperto circa 130 canali Telegram che vantano una notevole quantità di iscritti. Sono utilizzati per diffondere notizie e aggiornamenti pro-ISIS, ma anche per coordinare attentati.

Nel 2015 Pavel Durov ha affermato "il diritto alla privacy è più importante per Telegram della nostra paura che accadano cose brutte, come il terrorismo", ma in seguito agli attacchi di Parigi,

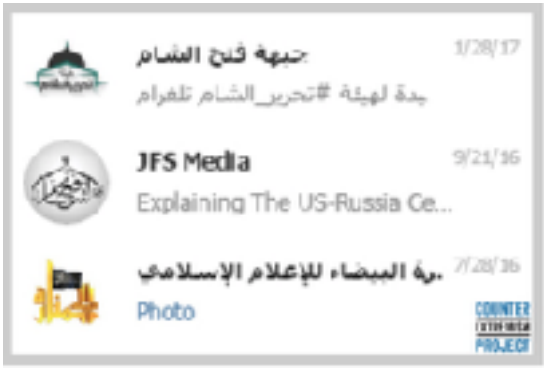
---

[21] https://faq.whatsapp.com/820124435853543/?helpref=uf_share

[22] tratto dalla lezione del Prof. Corrado Giustozzi, 14.03.2023

[23] الدولة الإسلامية في العراق والشام. "Stato islamico in Iraq e Siria"

del 13 novembre 2015, l'app di messaggistica si è impegnata a chiudere i canali pubblici dell'ISIS, anche se non sono intervenuti nell'eliminazione degli account personali.



Fonte: Counter Extremism Project

Amaq News Agency rappresenta il canale di informazione ufficiale dello Stato Islamico e vantava una presenza su tutte le piattaforme sociale e sui siti web tradizionali..

Dal 2016 a causa della censura subita, l'IS ha intensificato i suoi sforzi in materia di cybersecurity creando un vero e proprio help desk online impegnato in una guerra elettronica contro i sistemi di intelligence occidentali. La sua sede è Telegram.

Quest'app è certamente la preferita dagli estremisti, ma non l'unica. Secondo il rapporto 'Terrorist use of e2ee' di Tech Against Terrorism, infatti, ve ne sono altre. Tra le più famose, troviamo Whatsapp, We chat e Signal.

La preferenza dello Stato Islamico per Telegram si poggia sulla moltitudine di funzioni che mancano alle altre app, infatti essa gode di gruppi privati, super gruppi, canali e ampio limite di condivisione dei file.

Tuttavia, nonostante Telegram non presenti la crittografia end-to-end come opzione predefinita, a differenza di Whatsapp, essa ha una reputazione di app affidabile in materia di privatezza dei dati.

L'attendibilità dell'app risiede nella fiducia che gli utenti ripongono nell'indipendente CEO, Pavel Durov.

Durov è stato il fondatore del social network più in voga in Russia, VK. Nel 2010 ha perso il controllo della piattaforma, oltre che della cittadinanza russa, ora francese, proprio a causa del suo rifiuto di cedere i dati degli utenti ucraini al Cremlino.

Provando a mettere sinteticamente a confronto, dal punto di vista della crittografia delle chat, le due applicazioni di messaggistica più utilizzate possiamo riscontrare che:

1. il servizio e2e in Whatsapp è attivo di default e la piattaforma rassicura i suoi utenti nelle faq del sito web spiegando che, dal 2016, in nessun modo Whatsapp può vedere il contenuto dei messaggi o ascoltare le chiamate quando sono crittografati end-to-end[24]. Prosegue spiegando che la decrittazione dei messaggi inviati e ricevuti su WhatsApp avvengono interamente prima di lasciare dispositivo, momento in cui vengono protetti da un lucchetto apribile solo dal destinatario. La piattaforma più utilizzata al mondo continua chiarendo agli users che non conserva i messaggi una volta consegnati né i file di log delle transazioni di tali messaggi consegnati. Infine è possibile impostare un servizio di crittografia e2e anche per il backup[25], l'attivazione di tale funzione esclude la possibilità per Whatsapp e per Apple di accedere alla conversazione delle proprie chat.

2. Telegram ha scelto ad ogni costo di differenziarsi da Whatsapp, secondo Pavel Durov non così attenta alla privacy per diversi motivi:

- Nonostante sia possibile disattivare il backup delle chat non si può avere la certezza che anche il nostro interlocutore faccia lo stesso, l'accusa che il CEO di Telegram pone all'app di messaggistica instantanea (IM) concorrente è che questa si serva di terze parti per il backup delle chat degli utenti mentre Telegram utilizza i propri server.

- Telegram non voleva unirsi a quelle app IM "di nicchia" come le definisce il Durov[26] che non permettono di salvare i dati ed ha quindi lasciato libero arbitrio ai propri utenti offendo la possibilità di scegliere tra chat segrete (critografate e senza possibilità di accumulare dati e con eventuale possibilità di impostare un timer per la rimozione dei messaggi) e chat cloud.

- Un'altra differenza è rappresentata dal numero di telefono, Telegram obbliga gli utenti ad iscriversi con il numero di cellulare ma non è necessario utilizzarlo per avviare una chat, gli

[24] https://faq.whatsapp.com/820124435853543/?locale=it_IT

[25] https://faq.whatsapp.com/555895856296963/?helpref=hc_fnav&cms_platform=iphone&locale=it_IT

[26] https://telegra-ph.translate.goog/Why-Isnt-Telegram-End-to-End-Encrypted-by-Default-08-14?_x_tr_sl=en&_x_tr_tl=it&_x_tr_hl=it&_x_tr_pto=wapp

users possono servirsi di un *@username.* Anche questa funzione, come tutte le altre collegate alla privacy, è opzionale e non di default.

Una questione critica per entrambe le app IM è rappresentata dai Metadati, (luogo, data e ora di invio, numero di cellulare del mittente, indirizzo IP ecc) questi sono raccolti per un anno nei server di queste piattaforme a differenza di chat più sicure come Signal che li anonimizzano attraverso la crittografia[27].

CASE STUDY: ADEL KERMICHE

Adel Kermiche diciannovenne francese radicalizzatosi dopo essere entrato in contatto tramite Facebook con un gruppo jihadista ha provato a raggiungere la Siria in seguito agli attentati al giornale francese *Charlie Hebdo*, il 7 gennaio 2015.

Arrestato in Germania e rispedito in Francia ha aperto un canale Telegram nel quale ha condiviso un video con un compagno in cui i due giurano fedeltà allo Stato Islamico.

Il settimanale francese *l'Express* ha condiviso gli agghiaccianti messaggi audio del *mujaheddin*[28] inviati tramite il suo canale Telegram: "Prendi un coltello, vai in una chiesa e fai una carneficina. Tagli due o tre teste, poi è finita".

Il diciannovenne francese è uno degli attentatori alla chiesa di Saint-Etienne-du-Rouvray in Normandia nel luglio 2016.

Pochi minuti prima di entrare in chiesa ha effettuato l'ultimo accesso all'applicazione per invitare i suoi follower a condividere i contenuti che avrebbe pubblicato e, dopo aver ucciso Padre Hamel, ha costretto un ostaggio a registrare le conseguenze dell'attentato. Il video non è mai stato pubblicato poiché l'attentatore è stato ucciso da un agente di polizia durante l'assedio.

Adel Kermiche era collegato a Rachid Kassim[29], francese di origini algerine partito per la Siria nel 2012, amministratore di un canale Telegram che conta più di 300 iscritti nel quale condivide video di decapitazioni e manuali per realizzare attentati.

---

[27]https://www.cybersecurity360.it/soluzioni-aziendali/telegram-privacy-e-sicurezza-ecco-quanto-e-davvero-sicura/

[28] Combattente del Jihad

[29] Soren Seelow, "Rachid Kassim, le gourou des jeunes apprentis terror- istes," Le Monde, September 16, 2016.

In seguito alla morte di Kermiche, il suo profilo è stato riattivato, probabilmente da Rachid Kassim, per inviare audio, rimasti online per 10 minuti, nei quali un uomo si congratulava in francese con i suoi fratelli per le operazioni compiute.

2.4 Il Problema della Privacy nelle Transazioni con Criptovalute e il Terrorismo Islamico

Nel corso degli ultimi anni, il crescente interesse e l'adozione delle criptovalute hanno suscitato una serie di problematiche complesse, tra le quali si annovera il delicato equilibrio tra la sicurezza pubblica e la tutela della privacy nell'ambito delle transazioni finanziarie. Questo argomento ha suscitato particolari preoccupazioni riguardo al possibile utilizzo delle criptovalute da parte di gruppi terroristici, inclusi quelli con motivazioni di carattere religioso, al fine di finanziare le loro attività.

Le criptovalute presentano due caratteristiche chiave che alimentano queste preoccupazioni: l'anonimato e il pseudonimato. L'anonimato, ad esempio, è un aspetto particolarmente marcato in alcune criptovalute, come Monero e Zcash, che sono state appositamente progettate per garantire un elevato livello di segretezza nelle transazioni. Queste criptovalute utilizzano avanzate tecniche di crittografia per occultare gli importi delle transazioni e le identità dei mittenti e dei destinatari, rendendo estremamente difficile il loro tracciamento.

D'altra parte, criptovalute come Bitcoin e molte altre adottano il pseudonimato, dove le transazioni vengono registrate pubblicamente sulla blockchain, ma gli indirizzi delle criptovalute non sono direttamente collegati alle identità delle persone coinvolte. Gli utenti sono identificati solo attraverso una stringa alfanumerica, che funge da sorta di pseudonimo. Sebbene ciò offra un certo grado di privacy, non garantisce l'anonimato completo.

Le criptovalute presentano ulteriori vantaggi, tra cui la possibilità di effettuare transazioni transnazionali in modo rapido ed efficiente, superando le barriere geografiche e le restrizioni sui trasferimenti di denaro. Inoltre, poiché le transazioni avvengono su una blockchain decentralizzata, possono risultare più difficili da monitorare rispetto alle transazioni finanziarie tradizionali.

Tuttavia, l'uso delle criptovalute nel finanziamento del terrorismo solleva sfide significative per le autorità e le istituzioni finanziarie. Di conseguenza, stanno lavorando attivamente per sviluppare normative e linee guida che garantiscano la conformità alle normative AML (Anti-Money

Laundering) e KYC (Know Your Customer) da parte delle piattaforme di criptovalute. Questi requisiti sono essenziali per prevenire l'uso illecito delle criptovalute e garantire la legalità delle transazioni.

Inoltre, va considerato che l'interpretazione e l'applicazione della Sharia possono variare tra diverse comunità islamiche e tra studiosi religiosi. Ciò implica la possibilità di divergenze di opinione sul fatto che le criptovalute siano conformi o meno alla Sharia. Tuttavia, alcuni sviluppatori e aziende hanno intrapreso sforzi per creare criptovalute che rispettino i principi religiosi della Sharia. Ad esempio, sono stati sviluppati strumenti finanziari basati su blockchain che seguono i principi di profitto e perdita condivisi (Mudarabah e Musharakah), cercando di aderire alle normative islamiche.

In conclusione, la complessa relazione tra criptovalute, sicurezza pubblica e conformità alla Sharia solleva importanti questioni etiche e giuridiche. Tali questioni richiedono un approccio bilanciato per garantire la sicurezza pubblica senza compromettere eccessivamente la privacy e le libertà finanziarie dei singoli cittadini, considerando al contempo le leggi e le norme religiose pertinenti.

2.5 DARK WEB

Il dark web è la parte più nascosta di Internet, raggiungibile solo attraverso specifici software che garantiscono l'anonimato. La rete, o *darknet*, più famosa è Tor, altri esempi sono Freenet e I2P.

Tor nasce a metà degli anni Novanta con lo scopo di proteggere le comunicazioni tra i servizi segreti statunitensi e dal 2003 è stato reso pubblico.

La prima cosa che si nota entrando in Tor è che i siti specifici di questa rete non terminano con i tradizionali ".org/.com/.it …" bensì con ".onion" in riferimento al simbolo del software: la cipolla.

Tor, acronimo di The Onion Router, emula infatti la struttura di una cipolla nella gestione delle comunicazioni: l'anonimato è garantito da diversi strati di crittografia che vengono "sbucciati" durante la trasmissione. A differenza del surface web è estremamente difficile capire da quale indirizzo IP[30] sia partito un messaggio, perché prima di essere inviato al destinatario viene "rimbalzato" tramite diversi nodi della rete[31].

[30] Il protocollo che stabilisce gli standard e le regole per l'indirizzamento dei dati e la connessione a Internet

[31] Altri computer gestiti da utenti esterni

Il dark web, in costante crescita, è considerato da molti come un luogo pericoloso nel quale si svolgono attività illegali. Tuttavia, non è la tecnologia in sé ad essere pericolosa, bensì l'utilizzo che ne fa l'uomo.

La rete nascosta, come analizzato dal Professor Robert Gehl nel suo libro *"Weaving the dark web*[32]*"*, offre anche canali di comunicazione anonimi che garantiscono sicurezza e diffusione di news e reportage da parte di giornalisti o attivisti considerati oppositori di regime in ordinamenti sottoposti a tirannia.

Si pensi, ad esempio, alle rivolte popolari in Egitto nel 2011. Tor è stato utilizzato dagli attivisti dei diritti umani per nascondere le proprie attività su Internet affinché il regime di Mubarak non le censurasse.

Nonostante ciò, l'uso che si fa del "Web oscuro" nei paesi democratici è, in buona parte, quello di sviluppare atti illeciti.

Tra le attività illegali più famose troviamo vendita di droga e armi. Il tutto tramite i "mercati neri", veri e propri portali di e-commerce, il più celebre è Silk Road[33], chiuso nel 2015 dall'FBI.

Un caso tristemente noto di vendita di armi tramite il dark web riguarda l'attentato di Monaco del 22 luglio 2016, Ali Sonboly, diciottenne tedesco di origini iraniane, ha acquistato tramite criptovalute una Glock 17[34] e 200 munizioni servendosi del nome in codice "Mauracher".

Questo ambiente non monitorato ha permesso la proliferazione di gruppi jihadisti e l'instaurarsi di relazioni tra i reclutatori e coloro che sono inclini alla radicalizzazione.

Circola, ormai da diversi anni, una vera e propria letteratura jihadista disponibile solo online. Il nome di una delle più note riviste è Dābiq la cui prima pubblicazione è avvenuta nel corso del Ramadan 1435[35].

Essa prende il nome dalla città siriana citata nel ḥadīth[36] del Ṣaḥīḥ[37], località nella quale avrà luogo lo scontro finale tra bizantini ed Islam, che vedrà il trionfo di quest'ultimo sulla Terra.

---

[32] Weaving the Dark Web. Legitimacy on Freenet, Tor, and I2P. di Robert Gehl

[33] http://silkroad6ownowfk.onion (non più attivo)

[34] Pistola semiautomatica

[35] Secondo il calendario islamico equivale al luglio 2014

[36] Racconto di valore giuridico-religioso collegato alla vita del Profeta

[37] Ṣaḥīḥ al-Bukhārī è una raccolta di hadīth compilata da Abu Abdullah Muhammad Ibn Ismā`īl al-Bukhārī

Altri esempi di letteratura originatasi dai dotti di al-Qaeda sono *"Call for a Global Islamic Resistence"* e *"al-Battar"*. L'obiettivo di questi magazine è consentire una più ampia diffusione. Infatti, i testi classici non solo vengono facilmente tradotti in qualsiasi lingua occidentale, ma anche formattati in documenti Word ed E-Book.

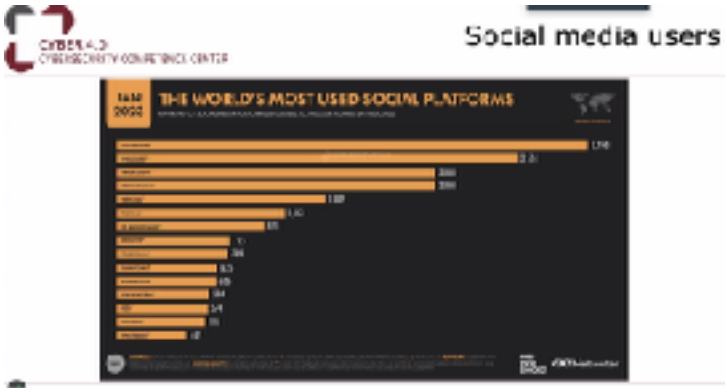
Dal 2016, in seguito alla vittoria dell'esercito turco a Daqib, queste riviste sono state sostituite in favore di Rumiyah, un nuovo magazine destinato alla pianificazione e allo svolgimento degli attentati.

Lo studio di questa rivista ha incoraggiato Abdul Razak Ali Artan, studente presso Ohio State University, a commettere l'omicidio di undici studenti presso il Campus seguendo le linee guida offerte dal magazine.

Il dark web è utilizzato per diffondere materiale finalizzato alla radicalizzazione proprio perché, a differenza del Surface web, mira a tutelare la vera identità degli utenti.

Tuttavia, nel suo report[38] già citato, Tech Against Terrorismsostiene che il Web di superficie sia il favorito dei terroristi dato che raggiunge un pubblico più vasto.

2.6 SOCIAL MEDIA



Grazie all'uso di queste piattaforme il pubblico è passato dall'essere un agente passivo all'essere attivo rispetto alla notizia. Questo perché, con la nuova tecnologia, è perfettamente in grado di raccogliere il materiale e di trarre una propria conclusione senza dover attendere la pubblicazione di una notizia su una testata giornalistica.

[38] TRENDS IN TERRORIST AND VIOLENT EXTREMIST USE OF THE INTERNET, 2022

L'estremismo islamico, come analizzato da Weimann nella sua opera *Web come teatro dell'orrore*, fin dai primi anni 2000 ovvero gli anni della nascita dei social media (Facebook viene fondato nel 2004 e Twitter nel 2006), si è servito delle piattaforme al fine di raccogliere fondi, pubblicare il proprio materiale e reclutare.

I ricercatori concordano sul fatto che le caratteristiche chiave di Internet – permettere l'invio e la ricezione di informazioni di volume maggiore e con una maggiore velocità di trasmissione, comunicazione bidirezionale e interattività - lo rendano differente dai media tradizionali.

Quando si tratta di utilizzare piattaforme come Twitter, l'Isis è "probabilmente più sofisticata della maggior parte delle società statunitensi", ha affermato Aaron Zelin, esperto di jihadisti e membro del Washington Institute.

Il crescente utilizzo dei social network da parte degli estremisti violenti ha portato la Quilliam Foundation, nel 2014, a produrre un rapporto intitolato *Trending Jihad* che analizza le principali piattaforme considerate a rischio radicalizzazione per i giovani.

La prima analisi riguarda le *chat room* e i forum che, a differenza dei siti Internet, danno la possibilità agli utenti di sviluppare nuove interazioni e mantenersi in comunicazione costante e per questo vengono utilizzate principalmente per il reclutamento.

Facebook, a causa dei meccanismi di tracciamento di cui dispone, non sembra essere utilizzato per pianificazioni dirette degli attentanti. Nonostante ciò, è spesso impiegato dagli estremisti per la diffusione di materiale come fotografie o riprese video.

Il suo utilizzo è largamente diffuso tra coloro che vogliono mostrare supporto ai gruppi jihadisti.

YouTube rappresenta la piattaforma streaming di video preferita dai gruppi estremisti. Secondo la Quilliam Foundation[39], non solo rende più difficile risalire all'identità dietro al canale che pubblica i contenuti, ma facilita anche l'interazione tra più soggetti nella sezione commenti situata sotto il materiale condiviso sulla piattaforma digitale.

Infine, il social media prediletto dai terroristi è Twitter, utilizzato soprattutto per interagire con celebrità, e con le maggiori autorità e, allo stesso tempo, provocarle pubblicamente. Infatti, tramite Twitter è possibile commentare apertamente eventi o personaggi noti nel panorama internazionale.

[39] Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it. By Ghaffar Hussain and Dr. Erin Marie Saltman

È proprio così che la guerra dello Stato Islamico avanza a colpi di Tweet, al punto che, il 16 giugno 2014, il Ministro delle comunicazioni iracheno è stato costretto a bloccare l'accesso a Internet[40] a tutta la popolazione, in seguito all'attacco alla base aerea di Camp Speicher[41] a Tikrit, in Iraq.

Un profilo affiliato all'ISIS ha rivendicato l'uccisione di 1700 sciiti[42] pubblicando 60 foto delle esecuzioni con didascalie annesse che deridono le vittime.

Non è stato un evento isolato. Nel corso del 2014, Internet è stato impiegato dallo Stato Islamico per rendere pubblici contenuti estremamente macabri. Ad esempio, è stato diffuso ampiamente il video che riprendeva la decapitazione del giornalista statunitense Steven Joel Sotloff[43].

Possiamo parlare di una vera e propria guerra dell'informazione iniziata nel 2014 e che prospera ancora oggi.

Daesh[44] si è trasformato in un esperto dello spazio digitale, del quale si serve per arricchire le file delle sue milizie.

Questo califfato virtuale genera potere essendo meno esposto alla presenza militare. Inoltre, sposta il conflitto su diversi fronti e funge da linfa vitale per quello Stato Islamico che sembrava essere quasi scomparso in Medio Oriente.

Secondo i dati emersi dal report del *National Consortium for the Study of Terrorism and Responses to Terrorism*, un centro di eccellenza del dipartimento americano di sicurezza interna presso l'Università del Maryland, Internet ha svolto un ruolo sempre più centrale anche nel contesto dei *Foreign Fighters.*

Un ruolo chiave nella radicalizzazione dell'83% dei combattenti stranieri è stato svolto proprio dalla Rete. Inoltre, è stata utilizzata per ottenere e fornire informazioni sul viaggio e sui metodi per evitare controlli alla frontiera.

---

[40] Iraq blocks Facebook and Twitter in bid to restrict Isis - BBC, Joe Miller

[41] https://www.hrw.org/news/2014/06/26/iraq-isis-execution-site-located

[42] Appartenente ad una delle sette musulmane risalenti al sec. I dell'egira, che riconoscono come soli eredi di Maometto i discendenti di suo genero, il califfo Alì.

[43] https://ent.siteintelgroup.com/Jihadist-News/is-behead-steven-joel-sotloff-threatens-to-execute-briton-david-cawthorne-haines.html

[44] الدولة الإسلامية في العراق والشام - al-Dawlah al-Islāmīyah fī al-`Irāq wa al-Shām- Stato Islamico in Siria e Iraq.

CASE STUDY: FACEBOOK JIHAD: analisi di discorsi e strategie di reclutamento rivolti a una donna occidentale[45]

Robin Toruk ha prodotto un interessante, anche se datato, report sul reclutamento online da parte di un gruppo jihadista nei confronti di una donna occidentale chiamata JFR.

Come abbiamo visto finora, c'è stato uno spostamento dell'attenzione dai campi di addestramento tradizionali alle piattaforme di Internet.

Il caso preso in considerazione riguarda l'analisi di un gruppo Facebook aperto anti-governativo per un periodo di tre mesi.

In prima istanza, il gruppo ha coinvolto JFR nella conversazione con temi a lei familiari, in questo caso il cristianesimo. Successivamente hanno provato a indurla a una conversione e, solo dopo aver raggiunto questo obiettivo, la hanno spinta verso la radicalizzazione servendosi di gentilezza, pazienza e identità di gruppo.

Attraverso i media occidentali, quali la rivista *Rolling Stone* online e *Reuters*, ma anche con piattaforme digitali come YouTube, hanno iniziato a condividere video e notizie di musulmani oppressi e bambini palestinesi vittime di abuso.

Da questo momento in poi nel gruppo Facebook si è iniziato a parlare della necessità di agire. In seguito all'apparente successo della conversazione, sono stati forniti alla donna una serie di collegamenti a siti web islamici radicali, quali http://www.ansar1.info e http://kavkazcenter.com/.

I post pubblicati successivamente hanno fatto riferimento ad Osama Bin Laden, leader di al-Qaeda, e Anwar al-Awlaki, considerato il più importante predicatore su Internet (i suoi video sono disponibili su YouTube).

In conclusione, hanno promosso discorsi di unità e martirio.

Questo studio evidenzia il modo in cui i social media stiano diventando strumenti sempre più potenti di reclutamento e mostra l'impiego che i terroristi fanno dei contenuti multimediali al fine di sollecitare una reazione da parte del soggetto target.

[45] Torok, Robyn, 'Facebook Jihad: A Case Study of Recruitment Discourses and Strategies Targeting a Western Female'. In: Proceedings of the Second International Cyber Resilience Conference, Perth: Edith Cowan University, 2011

2.6 FOREIGN FIGHTERS

I *foreign fighters* sono dei combattenti che scelgono di abbracciare la causa di un paese straniero impegnato contro un'altra fazione in una lotta politica o religiosa.

Circa 27.000 persone provenienti da tutto il mondo avrebbero lasciato le loro terre per raggiungere lo Stato islamico, secondo una dichiarazione del Ministro Marco Minniti[46] al centro studi americano nel luglio del 2017.

Secondo un'analisi condotta nel 2016 dal *National Bureau of Economic Research* il fenomeno sembra interessare principalmente 5 paesi: Tunisia, Arabia Saudita, Russia, Turchia e Giordania.

Tuttavia, anche l'Europa presenta questo problema: nel 2015 sono partite circa 5000[47] persone, di cui 48 di queste dall'Italia.

Quindi, seppur limitatamente, siamo parte integrante di questo processo.

Procedendo ora con un'analisi dei combattenti legati alla penisola si può notare che la maggior parte di essi è nata all'estero o da genitori stranieri.

Ad ogni modo, non mancano le eccezioni: tra i più noti cittadini italiani che hanno raggiunto il Califfato troviamo Lara Bombonati (condannata in Italia), Giuliano Delnovo (deceduto), Maria Giulia Sergio (deceduta) e Alice Brignoli[48] (arrestata nel 2021).

Lara Bombonati rappresenta un interessante caso di returnees[49]. Inoltre, come si può leggere dalla relazione al Parlamento del 2017 da parte del Ministero degli Esteri[50], il suo coinvolgimento con il gruppo terroristico *Hay'at Tahir al-Sham*[51] è emerso tramite i documenti contenuti nei suoi dispositivi elettronici.

Anche Whatsapp ha giocato un ruolo fondamentale in questa vicenda in quanto ha permesso l'arresto, da parte delle autorità belghe, del marocchino Chahed Chentouf Abdennaçar anch'egli impegnato nella causa jihadista.

---

[46] La Pagella Politica di Agi, Minniti ha ragione: ci sono 27mila foreign fighters dell'Isis. E alcuni torneranno, 21 luglio 2017

[47] Fonte: International Center for Counter Terrorism, Aja.

[48] https://www.europeandemocracy.eu/wp-content/uploads/2020/09/The-case-of-Alice-Brignoli-ENG-IT.pdf

[49] Reduci rientrati in Italia dopo essere partiti per lo Stato Islamico

[50] https://documenti.camera.it/_dati/leg18/lavori/documentiparlamentari/indiceetesti/038/001v02/00000032.pdf

[51] Organizzazione per la liberazione del Levante, conosciuto come al-Qaeda in Siria.

2.7 UNO SGUARDO D'INSIEME

In seguito alla battaglia di Baghouz, l'Occidente ha cantato vittoria credendo di aver sconfitto l'IS. Dal 29 giugno 2014, anno della proclamazione del Califfato, Daesh ha portato avanti le sue battaglie di Bāqiya wa Tatamaddad[52], come cita il suo motto.

Infiltrandosi nelle guerre civili irachena e siriana, lo Stato Islamico ha raggiunto la sua massima espansione nel 2015 quando è giunto fino in Libia usando a proprio favore la situazione instabile che si protrae dall'uccisione del Colonnello Muhammar Gheddafi avvenuta nel 2011.

Fin dagli albori, l'ISIS sfrutta le proprie abilità nell'utilizzo di Internet. Tutto è iniziato con la condivisione, il 19 agosto 2014, del suo primo video su YouTube: un uomo mascherato uccide il fotoreporter di guerra James Foley decapitandolo.

L'accurata propaganda mediatica dell'organizzazione terroristica prosegue attraverso filmati di esecuzioni e minacce all'Occidente, in particolare rivolte verso Roma.

Dal gennaio 2015 gli attacchi raggiungono l'Europa: Charlie Hebdo, la chiesa di Sant-Etienne in Normandia, il 22 marzo 2016 Bruxelles e ancora nel 2017 Manchester e Londra, per culminare con la Rambla a Barcellona.

Il sogno del Califfato globale sembrava inarrestabile fin quando la Syrian Democratic Forces (SDF), gruppo armato a guida curda e sostenuto dagli Stati Uniti, dichiarò di aver sconfitto lo Stato Islamico a Baghouz.

Nell'era digitale i l quarantacinquesimo Presidente degli Stati Uniti d'America, Donald Trump, non poteva che affermare la vittoria con un tweet.

[52] Consolidamento ed espansione

Tuttavia, questa notizia sembra essere solo parzialmente vera: questo è quanto si evince dai numeri di *foreign fighters* che ancora sostengono lo Stato Islamico e che testimoniano le loro battaglie in tempo reale sui social network.

In seguito alla pubblicazione del rapporto di *ICSR*[53] intitolato *#greenbirds* sono emersi importanti risultati sulla radicalizzazione tramite social network.

Il paese occidentale maggiormente colpito dal fenomeno dei combattenti stranieri, nel 2014, è il Regno Unito, seguito da Francia e Germania.

Chi sceglie di partire sembra essere già in contatto tramite Facebook o Twitter con promotori del jihadismo. I gruppi principali che utilizzano questi social network sono ISIS e Jabhat al-Nusrah.

A differenza di al-Qaeda, che sfruttava principalmente forum, tra i più famosi Ansar al Mujaheddin e as-Sahab, questi nuovi gruppi sunniti radicali hanno scelto, anche grazie all'ascesa di Twitter, di diffondere informazioni direttamente dal campo di battaglia pubblicando foto delle guerriglie, dei martiri e delle riunioni.

Un interessante dato emerso da questo report è che gli account dei predicatori, si pensi a Irhabi 007, sembrano essere più seguiti delle pagine ufficiali dei gruppi jihadisti. Questo per diverse ragioni: maggiori capacità linguistiche e visione d'insieme molto più ampia del quadro generale della Siria (a differenza dei combattenti che potrebbero non sapere cosa succede in un'altra città). Inoltre, i predicatori dedicano tempo all'interazione con la comunità digitale, mentre le pagine ufficiali si occupano esclusivamente della diffusione di notizie. Nel 2014 l'account più popolare su Twitter era quello di Shami Witness[54].

Ad ogni modo, anche le pagine pubbliche hanno un ruolo di rilievo nella radicalizzazione dei combattenti stranieri.

Con il passare degli anni è mutata perfino la figura del predicatore: ad oggi, la conoscenza delle lingue, il carisma e il numero di 'mi piace' ottenuti su Facebook sono elementi che rendono gli utenti un alfiere pari a Ayman al-Zawahiri[55].

---

[53] The International centre for the study of radicalization and political violence

[54] Shamiwitness, post su Twitter, 14 gennaio 2014, https://twitter.com/ShamiWitness/status/419613917300547585

[55] https://it.wikipedia.org/wiki/Ayman_al-Zawahiri#Gioventù

Si pensi alla nota figura di Ahmad Musa Jibril, nato in Michigan ma di origini palestinesi, prima di essere arrestato, affrontava temi come il Tawheed[56] e sosteneva la lotta armata contro il presidente siriano al-Assad tramite YouTube e Facebook.

I metodi, ai tempi non convenzionali, di quest'autorità religiosa gli hanno garantito un grande clamore mediatico e, anche se non direttamente, sembra essere il responsabile della conversione di molti combattenti stranieri.

Per concludere, il report ha evidenziato il ruolo centrale che hanno i social media nella decisione dei combattenti occidentali di partire per la Siria.

Queste piattaforme sono, per i *foreign fighters*, diventate essenziali in quanto rappresentano una fonte di ispirazione, informazione (danno la possibilità di condividere le proprie idee, ma anche di avere un feedback su come il conflitto venga percepito) e giustificazione grazie al supporto offertogli dai nuovi predicatori.

[56] Unicità di Dio

CAPITOLO 3

CONCLUSIONI

Come abbiamo evidenziato in questa analisi, nel periodo compreso tra il 2014 e oggi, i gruppi terroristici hanno progressivamente abbandonato i social media come canale di comunicazione, optando invece per applicazioni con crittografia end-to-end (e2e). Questa transizione è stata motivata dalla crescente domanda di privacy da parte degli utenti, che ha reso le app con crittografia e2e il principale mezzo di interazione.

Tuttavia, va notato che sei governi, tra cui Stati Uniti e Regno Unito, considerano pericolosa l'esistenza di queste piattaforme e hanno chiesto la creazione di cosiddette "backdoor," ossia meccanismi che consentano l'accesso alle conversazioni protette da crittografia. Questa controversia tra i decisori politici e i produttori di dispositivi digitali è emersa in seguito all'attacco terroristico di San Bernardino nel 2015, quando l'FBI ha richiesto senza successo ad Apple di sbloccare un iPhone 5.

Il cuore della questione riguarda la possibilità di intercettare le conversazioni: la richiesta dei politici di creare backdoor è stata interpretata da alcuni, come Edward Snowden[57], come un tentativo dello Stato di esercitare un controllo di massa sulla popolazione.

Gli obiettivi dei governi sono spesso legati alla sicurezza e alla protezione delle vittime, ma rimane incerto quali soggetti potrebbero necessitare di essere intercettati in futuro. Pertanto, sono state proposte due soluzioni[58] al problema:

1. L'introduzione di una vulnerabilità segreta, conosciuta solo dal programmatore, che consentirebbe una decodificazione delle comunicazioni in tempi ragionevoli.
2. L'adozione di un sistema di "key escrow," una cassaforte elettronica in cui vengono registrate le chiavi di crittografia fin dalla loro creazione.

È importante sottolineare che entrambe le soluzioni comporterebbero la perdita della privacy, poiché potrebbero portare a una caccia alla vulnerabilità nel primo caso o all'accesso alla cassaforte nel secondo.

---

[57] "Without encryption, we will lose all privacy. This is our new battleground", articolo su The Guardian del 15 ottobre 2019

[58] https://www.agendadigitale.eu/sicurezza/la-ue-e-il-ban-della-crittografia-contro-il-terrorismo-precedenti-rischi-possibili-soluzioni/

Per quanto riguarda la Commissione Europea, dopo aver analizzato i dati provenienti da una consultazione pubblica sul trattamento dei dati[59] personali e la privacy nel settore delle comunicazioni elettroniche, è stato emanato nel marzo 2021 un nuovo regolamento sulla protezione dei dati. Questo regolamento rafforza la privacy delle comunicazioni, considerandola un diritto fondamentale dei cittadini, e promuove lo sviluppo di una crittografia robusta e all'avanguardia, ritenuta essenziale nell'era digitale.

In questo contesto, è essenziale considerare anche il bilanciamento tra privacy e sicurezza nelle criptovalute. Le criptovalute offrono un alto grado di privacy grazie alla crittografia avanzata, ma questo può essere utilizzato sia per scopi legittimi che illeciti. Le sfide legate alla tracciabilità delle transazioni e alla prevenzione del finanziamento del terrorismo stanno spingendo le autorità a cercare un equilibrio tra la privacy degli utenti e la sicurezza pubblica.

Il fenomeno della radicalizzazione online ha subito un'evoluzione rapida e inarrestabile dagli inizi fino ad oggi. Inizialmente, il ruolo delle piattaforme utilizzate dagli estremisti è stato sottovalutato dai governi di tutto il mondo. Oggi, ci troviamo a combattere una guerra digitale senza confini definiti, con incertezza su quando e se possa essere risolta.

[59] https://edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_it.pdf

SITOGRAFIA

1. AGI, 6 giugno 2017. Ecco come l'Isis usa Telegram per fare propaganda. https://www.agi.it/estero/isis_terrorismo_telegram_social_network_jihadisti-1851029/news/2017-06-06/

2. ALTALEX, 25 Maggio 2021. Terrorismo sul web e contenuti online: il nuovo regolamento UE. https://www.altalex.com/documents/news/2021/05/25/terrorismo-web-contenuti-online-nuovo-regolamento-europeo

3. ALTALEX, 7 febbraio 2023, Dark web è tutto illecito? https://www.altalex.com/documents/news/2023/02/07/dark-web-tutto-illecito

4. Defence IQ, 4 ottobre 2017, Tools and tactics of radical Islamic groups hiding in the Dark Web Part I: Extremist Literature. https://www.defenceiq.com/cyber-defence-and-security/articles/tools-tactics-of-radical-islamic-groups-dark-web

5. Defence IQ, 7 novembre 2016, The modern way to undermine modern terrorism. https://www.defenceiq.com/defence-technology/articles/the-modern-way-to-undermine-modern-terrorism

6. https://cordis.europa.eu/article/id/394987-scouring-the-dark-web-for-terrorist-activity/it

7. https://www.consilium.europa.eu/it/policies/fight-against-terrorism/preventing-radicalisation/#radicalisation

8. https://www.dhs.gov/sites/default/files/publications/OPSR_TP_Overview-Profiles-Individual-Radicalization-US-Foreign-Fighters_508.pdf

9. IUS IN ITINERE, pubblicato 08/03/2023 · aggiornato 24/03/2023. Lotta al terrorismo per mezzo dell'Intelligenza Artificiale. https://www.iusinitinere.it/lotta-al-terrorismo-per-mezzo-dellintelligenza-artificiale-44054#_ftnref17

10. ISPI ONLINE, 6 novembre 2017. Disfatta ISIS e Foreign Fighters di ritorno: il caso italiano. https://www.ispionline.it/it/pubblicazione/disfatta-isis-e-foreign-fighters-di-ritorno-il-caso-italiano-18575

11. ISPI ONLINE, 14 Dicembre 2018, Le militanti italiane dello Stato Islamico. https://www.ispionline.it/it/pubblicazione/le-militanti-italiane-dello-stato-islamico-21796

12. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf

13. L'osservatore d'Italia, 7 aprile 2018, Cyberterrorismo, operazione Ansar: smantellato il canale isis su Telegram "Khilafah News Italia". https://www.osservatoreitalia.eu/cyberterrorismo-operazione-ansar-smantellato-il-canale-isis-su-telegram-khilafah-news-italia/

14. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/01/Gnosis-4-2015-teti.pdf

BIBLIOGRAFIA

15. Binder JF and Kenyon J (2022) Terrorism and the internet: How dangerous is online radicalization? Front. Psychol. 13:997390. doi: 10.3389/fpsyg.2022.997390

16. Burke J. The Age of Selfie Jihad: How Evolving Media Technology is Changing Terrorism «CTC Sentinel» 2016, volume 9

17. Carter J., Maher S., Neumann P. #Greenbirds: Measuring Importance and In uence in Syrian Foreign Fighter Networks. Department of War Studies, King's College London. 2014.

18. De Mutiis C. Verso una strategia italiana di prevenzione della radicalizzazione: una sfida globale che si vince a livello locale. Ministero degli Interni

19. Halava S., Frau-Meighs D., Hasan G. Youth and Violent Extremism on Social Media: mapping the research. UNESCO, Parigi, 2017

20. Hussain G. , Saltman E.M. Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it. Quilliam, 2014.

21. Marone, F. Digital Jihad. Online Communication and Violent extremism. ISPI, 2019.

22. Morisco V. Network jihadisti tra virtuale e reale. Sicurezza nazionale.gov.it, 2015.

23. M.G. Proli (2021) Prevenire i comportamenti antisociali e la radicalizzazione dei giovani attraverso Internet. L'esperienza del Progetto europeo "DIVE IN". Rief 18, 2: pp. 147-158. doi: https://doi.org/10.36253/rief-10653.

24. Savona P. , Vanorio F. Geopolitica dell'infosfera: l'eterna disputa tra Stato e mercato/individuo nel Nuovo Ordine Mondiale Digitale. Rubbettino editore, 2023

25. Schistad A. Self-radicalization on the internet. Steinerkskole, Oslo, 2021.

26. Sharda R. Dark Web. Exploring and Data Mining the dark side of the Web. Springer. Tuscon, AZ, USA, 2012.

27. Surace V. Il ritorno dei foreign terrorist fighters: l'evoluzione della disciplina giuridica per contrastare i rischi connessi ai returnees. Analytica for intelligence and security studies. Torino, 2020.

28. Thompson, Robin L.. "Radicalization and the Use of Social Media." Journal of Strategic Security 4, no. 4 (2012): 167-190. DOI: http://dx.doi.org/10.5038/1944-0472.4.4.8

29. Torok R. Facebook jihad: A case study of recruitment discourses and strategies targeting a Western female. 2nd International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 1st - 2nd August 2011.

30. Von Behr I., Reding A., Edwards C., Gribbon L. Radicalization in the digital era. The use of the internet in 15 cases of terrorism and extremism. RAND Europe, 2013.

31. Online gaming in the context of the fight against terrorism. Council of the European Union. Brussels, 2020.

32. Vidino L. Il jihadismo autoctono in Italia: nascita, sviluppo e dinamiche di radicalizzazione. ISPI. Milano, 2014.

Giorgia Pagliuca – *Laurea Triennale in interpretariato e traduzione con tesi sull'avvenire della Brexit, conseguita presso l'Università degli Studi Internazionali di Roma. Master in protezione del sistema paese presso SIOI. Attualmente studentessa magistrale in Criminalità, Investigazione e Sicurezza Internazionale, presso l'Università degli Studi Internazionali di Roma. Stagista presso Vision & Global Trends International Institute for Global Analyses, nell'ambito del progetto Società Italiana di Geopolitica.*

Analytical Dossier 08/2023
ISSN 2704-6419

Analytical Dossier 08/2023
ISSN 2704-6419

Vision & Global Trends - International Institute for Global Analyses

www.vision-gt.eu
info@vision-gt.eu