

## PREFAZIONE

### Come stoppare uno stato islamico online

Lo Stato Islamico, o ISIS, è il primo gruppo terroristico a detenere sia un territorio fisico che digitale: oltre alle strisce di terra che controlla in Iraq e Siria, domina le sacche di Internet con relativa impunità. Ma difficilmente sarà l'ultimo passo.

Sebbene ci siano ancora alcuni gruppi terroristici marginali nel Sahel occidentale o in altre aree rurali che non integrano digitalmente la loro violenza, è solo una questione di tempo prima che vadano online. In effetti, la prossima importante organizzazione terroristica avrà maggiori probabilità di avere estese operazioni digitali rispetto al controllo del terreno fisico. Giacché la battaglia militare contro l'ISIS sia innegabilmente una priorità assoluta, l'importanza del fronte digitale non dovrebbe essere sottovalutata. Il gruppo ha fatto ampio affidamento su Internet per commercializzare la sua ideologia velenosa e reclutare aspiranti terroristi. Secondo l'*International Center for the Study of Radicalization and Political Violence*, il territorio controllato dall'ISIS si colloca ora come il luogo con il maggior numero di combattenti stranieri dall'Afghanistan negli anni '80, con stime recenti che portano il numero totale di reclute straniere a circa 20.000, circa 4.000 dei quali provengono da paesi occidentali. Molte di queste reclute hanno avuto contatti iniziali con l'ISIS e la sua ideologia via Internet. Altri seguaci, nel frattempo, sono stati ispirati dalla propaganda online del gruppo a compiere attacchi terroristici senza viaggiare in Medio Oriente.

L'ISIS si affida anche alla sfera digitale per condurre una guerra psicologica, che contribuisce direttamente al suo successo fisico. Ad esempio, prima che il gruppo catturasse la città irachena di Mosul nel giugno 2014, ha lanciato una vasta campagna online con testo, immagini e video che hanno minacciato i residenti della città di morte e distruzione senza pari. Tale intimidazione rende più facile portare le popolazioni sotto il controllo dell'ISIS e riduce la probabilità di una rivolta locale. Sventare gli sforzi dell'ISIS su Internet renderà quindi il gruppo meno efficace sul campo di battaglia. Ad oggi, tuttavia, la maggior parte degli sforzi digitali contro l'ISIS sono stati troppo limitati, concentrandosi su tattiche

specifiche, come la creazione di controindicazioni all'estremismo, al posto di generare una strategia globale. Invece di ricorrere a un unico strumento, gli avversari dovrebbero trattare questa lotta come se fosse un confronto militare: intraprendendo una contro insurrezione su larga scala.

## **Conosci il tuo nemico**

Il primo passo di questa guerra digitale è capire il nemico. La maggior parte delle analisi dell'impronta online dell'ISIS si concentrano sui social media. In un rapporto della Brookings Institution, J. M. Berger e Jonathon Morgan hanno stimato che alla fine del 2014, 46.000 account Twitter hanno supportato apertamente il gruppo. All'epoca, le strategie per combattere l'ISIS online erano incentrate sulla semplice rimozione di tali account. Le piattaforme di social media sono solo la punta dell'iceberg, tuttavia. Gli strumenti di marketing di ISIS spaziano da piattaforme pubbliche popolari a chat room private a sistemi di messaggistica crittografati come WhatsApp, Kik, Wickr, Zello e Telegram. All'altra estremità dello spettro, case di produzione di media digitali come la Fondazione Al-Furqaan e il Media Center di Al-Hayat - presumibilmente finanziato e rispondendo alla leadership centrale dell'ISIS - sfornano video e pubblicità di livello professionale. La piena portata degli sforzi di marketing dell'ISIS senza sapere chi è dietro di loro non è un'intuizione attuabile; è come capire quanta terra controlla il gruppo senza sapere che tipo di combattenti la occupano e come la detengono. Un'efficace contro insurrezione richiede la comprensione della gerarchia dell'ISIS.

A differenza di al Qaeda, che comprende un ammasso allentato di cellule isolate, l'ISIS assomiglia a qualcosa di simile a una società. Sul terreno in Iraq e in Siria, una leadership altamente istruita stabilisce la sua agenda ideologica, uno strato manageriale implementa questa ideologia e un vasto grado e file contribuisce a combattenti, reclutatori, videografi, mogli jihadiste e persone con ogni altra abilità necessaria. Questa gerarchia viene replicata online, dove ISIS opera come una piramide composta da quattro tipi di ricerca digitali: in cima si trova il comando centrale dell'ISIS per le operazioni digitali, che dà ordini e fornisce risorse per la diffusione di contenuti. Sebbene i suoi numeri siano piccoli, le sue operazioni sono altamente organizzate. Secondo Berger, ad esempio, le origini

della maggior parte del materiale di marketing di ISIS su Twitter possono essere ricondotte a un piccolo gruppo di account con rigide impostazioni sulla privacy e pochi follower. Distribuendo i loro messaggi a una rete limitata al di fuori dell'opinione pubblica, questi account possono evitare di essere segnalati per violazioni dei termini di servizio. Ma il contenuto che rilascia alla fine scende al secondo livello della piramide: il rango e il file digitali dell'ISIS. Questo tipo di combattente può o meno funzionare anche offline. Lui e i suoi simili gestiscono account digitali collegati al comando centrale e diffondono materiale attraverso tattiche di guerriglia-marketing. Nel giugno 2014, ad esempio, i sostenitori dello Stato Islamico hanno dirottato gli hashtag di tendenza legati alla Coppa del Mondo per inondare i fan del calcio con la propaganda. Poiché operano in prima linea sul campo di battaglia digitale, questi combattenti spesso trovano i loro account sospesi per violazioni dei termini di servizio e possono quindi tenere account di backup. E per far apparire ogni nuovo account più influente di quanto non sia in realtà, acquistano follower falsi da società di social media marketing; solo \$ 10 possono aumentare il conteggio dei follower di decine di migliaia. Poi ci sono un gran numero di simpatizzanti radicali in tutto il mondo, che costituiscono il terzo tipo di traccia digitale ISIS. A differenza del grado e degli archivi, non appartengono all'esercito ufficiale dell'ISIS, non prendono ordini diretti dalla sua leadership o risiedono in Iraq o in Siria. Ma una volta attirati nel vortice dell'ISIS dal grado e dagli archivi, passano il loro tempo ad aiutare il gruppo a diffondere il suo messaggio radicale e convertire le persone alla sua causa. Queste sono spesso le persone che identificano e coinvolgono potenziali reclute a livello individuale, sviluppando relazioni online abbastanza forti da tradursi in viaggi fisici.

A giugno, ad esempio, il New York Times ha documentato in che modo un islamista radicale nel Regno Unito ha incontrato online una giovane donna dello Stato di Washington e l'ha convinta a prendere in considerazione di recarsi in Siria. Sebbene l'adesione alle operazioni dell'ISIS in Iraq e in Siria possa essere illegale, non lo è diffondere l'estremismo online. Questi combattenti sono maestri nel trarre vantaggio dal loro diritto alla libertà di parola e la loro forza risiede sia nel loro numero che nella loro volontà di imitare la linea ufficiale dell'ISIS senza dover ricevere ordini diretti dalla sua leadership. Il quarto tipo di ricerca digitale dell'ISIS è non umano: le decine di migliaia di account falsi che automatizzano la diffusione del suo contenuto e moltiplicano il suo messaggio. Su Twitter, ad

esempio, i cosiddetti bot di Twitter inondano automaticamente lo spazio digitale di retweet di messaggi terroristici; innumerevoli tutorial online spiegano come scrivere questi programmi relativamente semplici. Nelle sezioni dei commenti su Facebook, YouTube e altri siti, tali account automatici possono monopolizzare la conversazione con la propaganda estremista ed emarginare voci moderate. Questo esercito programmabile garantisce che qualunque contenuto di comando centrale digitale di ISIS si faccia strada attraverso il maggior numero di schermi possibile.

## **Ricostruzione del territorio digitale**

Gran parte del dibattito su come combattere l'ISIS sul suo terreno è stato binario, diviso tra coloro che propongono il contenimento e quelli che insistono sulla sua sconfitta. La migliore strategia per combatterla online, tuttavia, è qualcos'altro: emarginazione. Il risultato sarebbe qualcosa di simile a quello che è successo alle Forze armate rivoluzionarie della Colombia, o FARC, il gruppo narcoterrorista che ha conquistato titoli negli anni '90 per i suoi rapimenti di alto profilo e la selvaggia lotta di guerriglia. Oggi, il gruppo non è stato sciolto né completamente sconfitto, ma i suoi ranghi sono stati in gran parte portati nella giungla. Sulla stessa linea, l'ISIS verrà castrato come una minaccia digitale quando la sua presenza online diventerà appena percettibile. Il gruppo troverebbe troppo rischioso o tatticamente impossibile ottenere il controllo delle piattaforme dei social media e delle chat room pubbliche e il suo contenuto digitale sarebbe difficile da scoprire. Incapace di far crescere i suoi ranghi online, vedrebbe il suo rapporto tra combattenti digitali e combattenti umani cadere a uno a uno. Sarebbe costretto a operare principalmente sul cosiddetto Web oscuro, la parte di Internet non indicizzata dai motori di ricerca tradizionali e accessibile solo agli utenti più esperti. Le convincenti organizzazioni terroristiche a operare in segreto rendono le trame più difficili da intercettare, ma nel caso dell'ISIS, vale la pena fare un compromesso.

Ogni giorno, il messaggio del gruppo raggiunge milioni di persone, alcune delle quali diventano sostenitori dell'ISIS o addirittura combattenti per la sua causa. Impedirgli di dominare il territorio digitale aiuterebbe a bloccare il rifornimento dei suoi ranghi fisici, ridurre il suo impatto sulla psiche pubblica e distruggere i suoi mezzi di comunicazione più fondamentali. Ci vorrà un'ampia coalizione per

emarginare l'ISIS online: dai governi e dalle società alle organizzazioni non profit e alle organizzazioni internazionali. Innanzitutto, dovrebbero separare gli account gestiti dai social network da quelli automatizzati. Successivamente, dovrebbero concentrarsi sul comando centrale digitale dell'ISIS, identificando e sospendendo i conti specifici responsabili della definizione della strategia e impartendo ordini al resto del suo esercito online. Fatto ciò, la società digitale in generale dovrebbe spingere il livello e i file rimanenti nell'equivalente digitale di una caverna remota. La sospensione degli account deve essere mirata, più come i raid di uccisione o cattura che le campagne di bombardamenti strategici. Le sospensioni generali che coprono tutti gli account che violano i termini di servizio non potrebbero garantire che la leadership sarà influenzata. In effetti, come evidenziato dalla ricerca di Berger e Morgan, l'ISIS ha imparato a proteggere la sua leadership digitale dalla sospensione mantenendo le sue attività nascoste dietro rigide impostazioni sulla privacy. Ciò non significa minimizzare l'importanza di vietare agli utenti che infrangono le regole e distribuiscono contenuti terroristici. Le aziende tecnologiche sono diventate abili nel fare proprio questo.

Nel 2014, l'unità di segnalazione Internet britannica antiterrorismo, un servizio gestito dalla polizia metropolitana di Londra, ha lavorato a stretto contatto con società come Google, Facebook e Twitter per contrassegnare oltre 46.000 pezzi di contenuti violenti o odiosi da rimuovere. Nello stesso anno, YouTube ha eliminato circa 14 milioni di video. Nell'aprile 2015, Twitter ha annunciato di aver sospeso 10.000 account collegati all'ISIS in un solo giorno. Tali sforzi sono preziosi in quanto forniscono un ambiente digitale più pulito a milioni di utenti. Ma lo sarebbero doppiamente se venisse eliminata anche la leadership che ordina la distribuzione di contenuti terroristici. Ciò, a sua volta, richiederà la mappatura della rete di account ISIS. Un modo in cui le forze dell'ordine potrebbero farsi strada in questa rete digitale è infiltrarsi di nascosto nella rete del mondo reale dell'ISIS. Questa tecnica ha già ottenuto un certo successo. Ad aprile, l'FBI ha arrestato due giovani donne accusate di aver pianificato attacchi a New York City dopo un'indagine di due anni che aveva fatto ampio affidamento sulla loro attività sui social media come prova. Le forze dell'ordine dovrebbero aumentare tali sforzi per concentrarsi sul dominio digitale e indirizzare la leadership digitale dell'ISIS, sospendere i conti dei suoi membri e arrestarli in alcuni casi. Una volta che la leadership online dell'ISIS è stata separata dal grado e dal file diventerà

significativamente meno coordinato e quindi meno efficace.

Il prossimo passo sarebbe quello di ridurre il livello di attività online del gruppo in generale, in modo che sia costretto ai margini della società digitale. Durante questa fase, il pericolo è che online, l'ISIS possa frammentarsi in gruppi canaglia meno coordinati ma più aggressivi. Con una maggiore tolleranza per il rischio, questi gruppi potrebbero intraprendere il *doxing* degli oppositori dell'ISIS, in base al quale vengono rivelate le informazioni private (come l'indirizzo e il numero di previdenza sociale) di un bersaglio, o attacchi di negazione del servizio distribuito, che può distruggere un intero sito Web. Per mitigare questa minaccia, le attività dei combattenti digitali devono essere completamente allontanate dall'estremismo. È qui che possono entrare in gioco le controindicazioni dell'estremismo violento.

Negli ultimi due anni sono stati lanciati numerosi sforzi notevoli, tra cui la serie video prodotta dal Centro arabo per la ricerca scientifica e gli studi umani e dall'Istituto per il dialogo strategico. Per essere efficaci, queste campagne devono riflettere la diversità dei ranghi del gruppo: combattenti jihadisti professionisti, ex soldati iracheni, studiosi islamici profondamente religiosi, giovani in cerca di avventura, residenti locali che si uniscono per paura o ambizione. Moderati messaggi religiosi possono funzionare per la pia recluta, ma non per la sola cellula adolescente britannica a cui sono state promesse mogli multiple e un senso di appartenenza alla Siria. Potrebbe essere meglio usare qualcosa di più simile alle campagne di prevenzione del suicidio e anti-bullismo. Per ottenere il massimo effetto, queste campagne devono essere attentamente mirate.

Un video anti-estremista visto da 50.000 persone del giusto tipo avrà un impatto maggiore di quello visto da 50 milioni di spettatori casuali. Prendiamo ad esempio Abdullah-X, una serie di cartoni animati commercializzata attraverso una campagna YouTube finanziata dall'Unione Europea.

Il suo episodio pilota è stato promosso usando una pubblicità mirata orientata verso coloro che erano interessati all'Islam estremista. L'ottanta per cento degli utenti di YouTube che l'hanno visto lo ha trovato attraverso annunci mirati piuttosto che attraverso ricerche non correlate. Data la diversità del rango e dei file digitali dell'ISIS, tuttavia, scommettere solo sulle controindicazioni sarebbe troppo rischioso. Per combattere gli estremisti che hanno già deciso, la coalizione dovrebbe mirare alla loro volontà di operare all'aperto.

Al Qaeda ha fatto tutto il possibile per mantenere segrete le sue operazioni

digitali e lavora sotto copertura di password, crittografia e rigide impostazioni della privacy. Queste tattiche hanno reso il gruppo notoriamente difficile da tracciare, ma hanno anche mantenuto la sua minuscola impronta digitale. Allo stesso modo, il rango e i file ISIS dovrebbero essere costretti ad adottare un comportamento simile. Raggiungere questo richiederà creatività. Ad esempio, i governi dovrebbero prendere in considerazione la possibilità di lavorare con i media per pubblicizzare in modo aggressivo gli arresti risultanti da infiltrazioni segrete della rete online dell'ISIS. Se un nuovo account con cui un soldato digitale interagisce comporta il rischio di essere quello di un agente sotto copertura, diventa esponenzialmente più pericoloso assumere nuovi membri. Le forze dell'ordine potrebbero anche creare presentazioni visive che mostrano come le indagini della polizia sui conti degli estremisti digitali possano portare ad arresti, raccontando così la storia cautelativa che un singolo errore può causare la caduta di un soldato digitale e del suo intero social network.

Entro i prossimi anni, potrebbero diventare disponibili nuovi strumenti ad alta tecnologia per aiutare i governi a emarginare i terroristi digitali. Uno è l'apprendimento automatico. Proprio come gli inserzionisti online possono indirizzare gli annunci agli utenti con un particolare insieme di interessi, le forze dell'ordine potrebbero utilizzare l'analisi algoritmica per identificare, mappare e disattivare gli account dei sostenitori del terrorismo. Assistiti dall'apprendimento automatico, tali campagne potrebbero combattere l'ISIS online con una precisione ritrovata e raggiungere una scala che non sarebbe possibile con un approccio manuale. Vale la pena notare che proprio come una contro insurrezione fisica, una contro insurrezione digitale ha maggiori probabilità di successo se sostenuta dalla partecipazione delle comunità locali. Tutte le piattaforme online che ISIS utilizza hanno moderatori di forum, l'equivalente di leader tribali e sceicchi. Le società tecnologiche che possiedono queste piattaforme non hanno interesse a vedere i loro ambienti inondati di account falsi e messaggi violenti. Dovrebbero quindi fornire a questi moderatori gli strumenti e la formazione per proteggere le loro comunità dalla messaggistica estremista. Anche in questo caso, l'apprendimento automatico potrebbe un giorno aiutare, identificando automaticamente i messaggi terroristici e evidenziandoli per i moderatori o bloccandoli per loro conto.

## **Accesso negato**

A prima vista, l'ISIS può sembrare irrimediabilmente dominante online, con il suo esercito persistente di venditori ambulanti di propaganda e troll automatizzati. In realtà, tuttavia, il gruppo è in netto svantaggio quando si tratta di risorse e numeri. La stragrande maggioranza degli utenti di Internet non è d'accordo con il suo messaggio e le piattaforme utilizzate dai suoi combattenti appartengono a società che si oppongono alla sua ideologia. Non c'è dubbio che intraprendere una campagna di contro insurrezione digitale rappresenti un territorio inesplorato. Ma i costi del fallimento sono bassi, poiché a differenza di una contro insurrezione nel mondo reale, coloro che combattono digitalmente non corrono rischi di lesioni o morte. Questo è un altro fattore che rende l'ISIS particolarmente vulnerabile online, poiché significa che gli avversari del gruppo possono applicare e scartare rapidamente nuovi modi di combattere il terrorismo per affinare la loro strategia. I vantaggi dell'emarginazione digitale dell'ISIS, nel frattempo, sono molteplici. Non solo castrare il gruppo online migliorerebbe la vita di milioni di utenti che non avrebbero più la probabilità di incontrare la propaganda del gruppo; renderebbe anche la sconfitta del mondo reale del gruppo più imminente. Man mano che le piattaforme digitali, i metodi di comunicazione e i soldati dell'ISIS diventassero meno accessibili, il gruppo troverebbe più difficile coordinare i suoi attacchi fisici e ricostituire i propri ranghi. E quelli che lo combattono online avrebbero acquisito una preziosa esperienza per quando sarebbe arrivato il momento di combattere il prossimo gruppo terroristico globale che cercava di conquistare Internet.

## **Come combattere una Nazione che non esiste**

Giuseppe Paccione spiega perfettamente come l'ISIS non sia mai stato riconosciuto dalla comunità internazionale come un vero e proprio Stato, pur avendo creato apparati istituzionali alla pari di altri Stati, con confini precisi. Paccione approfondisce la storia, accompagnato dall'aspetto prettamente giuridico internazionale *in primis* la questione dell'uso della forza militare al di là della Carta delle Nazioni Unite e del diritto internazionale generale che inibisce tale strumento bellico, tranne che per legittima difesa.

Racconta la nascita di un Paese (allora costituito da territori dell'Iraq e della



Siria conquistati dai membri dell'ISIS), autoproclamatosi Califfato, che non c'è. Spiega come affrontarlo. Di come superare la paura. Paccione analizza, infine, precisamente il fenomeno dell'ISIS e spiega come diplomazia, analisi dei dati, controlli e aiuti *in loco* siano le vere armi per vincere una guerra che non viene combattuta solo con le armi tradizionali.

Settembre 2022

Gian Nicola Pittalis\*

\* Gian Nicola Pittalis, nato a Sassari nel 1974, è giornalista professionista con alle spalle diverse pubblicazioni. Esperto in cultura, sport, cronaca nera, collabora con alcune delle testate nazionali più importanti. Tra i suoi libri "I Grandi Condottieri della Serenissima", "L'Inquisizione a Venezia", "Se tutti gli chef sono in televisione, noi andiamo in trattoria" con Arrigo Cipriani. Direttore di testate on line è anche conduttore televisivo.