31/03/2020

DEEP WEB E TERRORISMO
LA COMPONENTE INFORMATICA NEL MODERNO TERRORISMO

Di Raffaele Olla

GENESI DELLA RELAZIONE TRA WEB E TERRORISMO

Viviamo nella cosiddetta Industria 4.0. Le nuove tecnologie hanno già un profondo impatto nella vita quotidiana e l'apporto tecnologico non potrà che diventare sempre più basilare nella Nostra vita.

Il terrorismo odierno, diversamente da quello degli anni '70 e '80, si è adattato ai processi evolutivi sfruttando la componente tecnologica. Il cyberspazio è per genesi privo di confini, un luogo privilegiato dove i terroristi possono trovare le risorse necessarie alle proprie attività, fare propaganda, lanciare attacchi fisici e informatici contro i proprio nemici, reclutare nuovi adepti e commerciare con alter ego digitali.

"*Gli attacchi terroristici sono spesso preparati meticolosamente per dare il massimo risalto agli eventi. Presentano "coreografie" studiate per massimizzare l'attenzione dei media. Il terrorismo oggi è pianificato per coinvolgere non solo le vittime, ma anche coloro che assistono. Il terrorismo è un teatro* ", ha scritto l'esperto internazionale di terrorismo Brian Jenkins.[1]

Tra le principali organizzazioni terroristiche attive sul web ci sono Hamas, Hezbollah, Al-Gama'a al Islamiyah, il PKK, l'Esercito zapatista di Liberazione Nazionale (ELNZ), il Movimento Islamico dell'Uzbekistan (IMU) Mujahedin, l'ISIS e i ceceni.

1https://www.yumpu.com/it/document/read/55712064/terrorismo/3

Nell'analisi di Brian Jenkins si definiva il rapporto costante ed evolutivo tra terrorismo e web già dal 1998 quando i primi siti web di matrice terroristica incominciavano a fare propaganda anche tramite canali non convenzionali.

Internet è di facile accesso da qualunque parte del mondo, un terrorista può raggiungere istantaneamente grandi platee oppure indirizzare i propri messaggi a specifici gruppi di individui.

Con opportuni accorgimenti, è possibile operare nel completo anonimato, un grande vantaggio per un'organizzazione terroristica intenta in attività di propaganda.

L'aspetto che rende Internet uno strumento ideale per i gruppi terroristici è che è economico ed è interattivo.

Per la prima volta nella storia i gruppi terroristici possono interagire in tempo reale con i loro simpatizzanti. La vera forza degli attacchi terroristici cui stiamo assistendo è l'effetto di amplificazione ottenuto attraverso i social media.

Internet, e in generale la tecnologia, sono sfruttati da organizzazioni terroristiche per diversi scopi, tra cui:

- Propaganda
- Guerra psicologica
- Reclutamento e mobilitazione
- Fundraising, raccolta di fondi per iniziare un progetto, un'attività
- Data Mining, raccolta di informazioni
- Comunicazioni protette
- Attacchi informatici
- Distribuzione del software (ad esempio, mobile app)
- Acquisto di documenti falsi
- Formazione

Le attività di propaganda in Internet rappresentano l'uso più comune della tecnologia da parte delle organizzazioni terroristiche. Gruppi come l'ISIS hanno dimostrato una grande padronanza della tecnologia e una profonda conoscenza delle moderne tecniche di comunicazione.

Ogni video è preparato con cura, e la sua programmazione è meticolosa e finalizzata al raggiungimento del maggior numero di individui.

I terroristi usano le nuove piattaforme social come Facebook, Twitter e social media come YouTube. Il loro linguaggio è diretto, accattivante, giovane, e può raggiungere un pubblico specifico utilizzando immagini ad alto impatto emotivo.

L'effetto di amplificazione si ottiene attraverso la facile diffusione di contenuti in rete attraverso le stesse piattaforme social, servizi di messaggistica istantanea (Telegram su tutte) ed applicazioni mobili.

A lato del cosiddetto web di superficie o clear web, esiste, tuttavia, la sua parte sommersa conosciuta come deep web (in genere raccoglie blog e attività legate ad informazioni provenienti da Paesi dove esiste una forte cintura alla libertà di comunicazione oppure sistemi crittografati di

comunicazione) e sempre più in profondità il dark web o dark net[2] (la parte più oscura della rete in quanto fonte di dati di matrice terroristica o di altre attività criminali come la pedopornografia).

2La denominazione *net* poichè non è prevista il comune protocollo *http://* usato invece nel web

IL CYBER TERRORISMO

A coniare il termine cyber terrorismo fu negli anni ‘80 il ricercatore dell'Institute for Security and Intelligence (California) Barry Collin nel mettere in chiaro la stretta relazione che stava nascendo tra il terrorismo e l'ambiente del cyber-spazio. Mentre nella decade successiva il dibattito si allargherà all'*information warfare*, in quel periodo la discussione era incentrata sul *cyber terror* e sul nuovo modo di concepire il mondo, alla luce dei rischi provenienti dalle nuove tecnologie.

Molte figure associano l'organizzazione del terrorismo alla rete del darknet ma, contrariamente a quanto si potrebbe pensare, le reti anonime come Tor[3] e I2P non sono i luoghi informatici preferiti dalle organizzazioni terroristiche.

Lo sostengono diversi studi a riguardo. D’altra parte, le forze dell’ordine e i servizi segreti temono giustamente che il rafforzarsi dello Stato Islamico possa essere associato ad un uso crescente delle reti anonime e del fatto che queste rendono le indagini difficili.

Poche ore dopo gli attacchi di Parigi del 13 novembre 2015, gli esperti di sicurezza hanno trovato sulla rete Tor un nuovo hub di propaganda. Il sito includeva la traduzione in inglese, turco e russo di contenuti condivisi dai membri del Daesh, legati proprio agli attacchi di Parigi. Gli esperti hanno notato un post che spiegava la necessità di creare un nuovo hub per la propaganda. Probabilmente, questa è la risposta alle numerose operazioni contro altri siti web utilizzati dall’ISIS, sequestrati dalle forze dell’ordine e seguiti da hacktivisti on-line.

Un altro problema, quando si tratta di reti anonime, è quello riguardante la loro non stabilità e frequente lentezza.

Questo non significa che i terroristi non usino il Dark Web: al contrario, gli esperti hanno evidenziato che i militanti di gruppi come l’ISIS comunemente usano Tor per rendere anonima la navigazione proprio su Internet.

“*La propaganda che corre sul darknet è rigidamente limitata, anche perché i principianti possono essere scoraggiati dalla illegalità nella fase iniziale, al contrario di un più semplice e curioso Googling*”, si legge nello studio. “*I servizi nascosti, in secondo luogo, spesso non sono stabili o abbastanza accessibili per una comunicazione efficace; altre piattaforme sembrano soddisfare le esigenze di comunicazione* “.

I terroristi usano il web per la propaganda e il reclutamento: due obiettivi facilmente massimizzati utilizzando piattaforme social media come Twitter e Facebook. La ricerca, infatti, conferma che il

3E’ un software libero che permette una comunicazione anonima per il web e per il deep web

Dark Web ospiti una parte significativa dei servizi utilizzati dalle organizzazioni criminali per proporre i loro prodotti e servizi, tra cui “la droga, la finanza illegale e la pornografia spesso affiancata alla violenza sui bambini e sugli animali”.

LA E-JIHAD

L'innovazione più significativa apportata dallo Stato Islamico riguarda la comunicazione, che vede team dall'Africa occidentale all'Afghanistan lavorare senza sosta per diffondere il "brand" del califfato.

Le sue strategie comunicative sono state approfonditamente analizzate dal report del ricercatore della Quillam Foundation, Charlie Winter. Secondo lo studio, il califfato rilascia in media 38 slot di propaganda al giorno, tra foto, audio, video e testi, rendendo vane misure repressive come la censura. Anche il tentativo di trovare una contro-narrativa per esautorare il brand del gruppo è fuori luogo, in quanto dovrebbe piuttosto essere elaborata una narrativa.[4]

É fondamentale sottolineare che, a dispetto di quanto riportato dai giornali e politici occidentali, la violenza non è l'unico contenuto della produzione mediatica dello stato islamico. I temi principali classificati dallo studio sono pietà, appartenenza, brutalità, vittimismo, guerra e utopia. Più della metà dei contenuti si focalizza sulla vita dei civili nei territori occupati dall'ISIS, descrivendo uno scenario fatto di attività economiche, eventi sociali, ordine pubblico e fervore religioso. In questo modo, il gruppo attrae sostenitori sia dal punto di vista ideologico che politico.

Allo stesso tempo, la propaganda insiste molto sul tema della guerra e delle operazioni militari, arrivando a mettere in scena dei falsi attacchi per perpetuare l'idea che lo stato Islamico sia costantemente sull'offensiva.

Il pubblico a cui esso si rivolge, tuttavia, è più regionale rispetto al passato, con l'obbiettivo di scoraggiare il dissenso e gli atti di ribellione nei territori controllati dal califfato. In quanto ai mezzi di diffusione, in passato i gruppi jihadisti tendevano a prediligere i forum in lingua araba protetti da una password per comunicare e scambiarsi idee. Tali forum sono ancora attivi ma hanno assunto un ruolo secondario rispetto ai social media open source e peer to peer, grazie ai quali il gruppo ha registrato un successo senza precedenti nel recruitment.

4Orsini, Alessandro. “ISIS: I terroristi più fortunati del mondo e tutto ciò che è stato fatto per favorirli”. (Milano: Rizzoli, 2016)

Dati i problemi etici e legislativi causati dall'uso delle loro piattaforme, le grandi corporation hanno reagito con forza. Facebook, per esempio, ha introdotto una stretta regolamentazione che ha permesso di espellere la propaganda jihadista dalla piattaforma. Lo stesso non si può dire di Twitter, che fatica ancora a raggiungere questo obbiettivo. A partire dall'estate 2014, lo stato islamico ha smesso di utilizzare account ufficiali, perché più facili da individuare e sospendere, operando soprattutto attraverso gli hashtag. Questi ultimi non possono essere né bloccati né sospesi da Twitter e consentono di raggiungere in poco tempo una vastissima diffusione.

QUALI I PERICOLI E QUALI I MEZZI DI CONTRASTO AL FENOMENO DEL CYBER TERRORISMO

Il Dark Web, come abbiamo visto, è un ambiente difficile da monitorare per ammissione stessa degli esponenti delle agenzie di intelligence e delle forze dell'ordine, è naturale quindi che cellule terroristiche lo utilizzino per le proprie attività.

«Alcuni hidden service – spiegano dal Clusit[5] – presenti nella rete TOR sono stati utilizzati come repository degli eseguibili di mobile app utilizzate da gruppi jihadisti per comunicazioni sicure. Abbiamo notizia di alcuni siti utilizzati per condividere indirizzi Bitcoin per la raccolta di fondi per finanziare attività delle cellule operative in occidente. In rete è reperibile il testo "*Bitcoin wa Sadaqat al Jihad*" che spiega come acquistare armi nel dark web per azioni terroristiche.

Le darknet sono state anche utilizzate per diffondere un manuale, intitolato "*How to Tweet Safely Without Giving out Your Location to NSA*" che istruisce i militanti dell'ISIS a eludere le attività di sorveglianza operate dalle agenzie di intelligence occidentali».

Gli esperti hanno condotto un singolare esperimento: una volta identificate 8.707 pagine "sospette" hanno analizzato i link contenuti in queste pagine e che referenziavano contenuti nelle darknet.

I contenuti dei siti web presenti nel dark web sono risultati i seguenti:

- Siti utilizzati per la distribuzione di malware (drive-by download) (33.7%)
- Siti per anonimizzare la navigazione in rete (31.7%)

5CLUSIT (Associazione Italiana per la Sicurezza Informatica)

- Siti contenenti materiale Pedopornografico (26%)

Nel luglio 2015, l'Europol ha lanciato l'unità *Internet Referral* per combattere la propaganda terroristica su Internet. Essa si propone i seguenti obiettivi:

- coordinare e condividere i compiti di identificazione e segnalazione dei contenuti di matrice terroristica;

- effettuare e supportare, in modo efficiente ed efficace, i rinvii;

- sostenere le autorità competenti, fornendo analisi strategiche e operative;

- agire come Centro europeo di eccellenza per i compiti sopra elencati

Secondo il direttore di Google Ideas, Jared Cohen, sarebbe necessario confinare i gruppi terroristici, come l'ISIS, nel Dark Web, dove la loro propaganda non avrà la stessa facilità diffusiva.

Inoltre, propone di cancellare immediatamente i loro account, così che le persone non possano entrarvi in contatto.

A scendere in campo contro l'ISIS non sono solo le istituzioni governative ma troviamo anche gli hacker, come ad esempio gli *Anonymous*.

La campagna più attiva, che ha più che altro lo scopo di informare, è *#opIceIsis*, che gira intorno a due account Twitter: @TheAnonMessage e @OpIceIsis.

Infatti, in un'intervista a *France2419*, un membro del gruppo ha spiegato le motivazioni dietro questa campagna, ovvero sottolineare la responsabilità degli USA nella nascita dell'ISIS, ribadire che la religione islamica non è quella di cui si fa interprete lo Stato Islamico e mostrare ciò che accade in Iraq. Troviamo anche *The Jester*, un gruppo di hacker filo-americani e filo-governativi, da sempre nemici di Anonymous, che sono riusciti a far chiudere numerosi profili di militanti o simpatizzanti ISIS. Un esempio è anche il gruppo turco *RedHack* di ispirazione marxista-leninista, molto vicino ad Anonymous e ai curdi, quindi profondamente anti-ISIS.

L'attacco hacker post-attentato di Parigi rientra in un più vasto progetto di Anonymous, che prevede l'annientamento dell'Isis su internet, anche sul Deep Web, dove ora i terroristi stanno reclutando nuove persone da immolare nel Jihad.

E mentre Isis posta immagini di miliziani neri che sventolano drappi neri, hacker con indosso la maschera di *V per Vendetta* li sbeffeggiano, modificando quelle fotografie con personaggi manga intenti a tagliare meloni invece di teste o con messaggi ironici come i meme di “Isis minaccia”, diventati un tormentone sui social, o trasformandoli in paperelle di plastica.

Quando l'ironia ferisce più di una spada.

LUPI SOLITARI MA NON COSÍ SOLITARI

E se i lupi solitari fossero meno solitari di quanto si pensi?

Il killer di Nizza Mohamed Bouhlel, l'aggressore con l'ascia di Wurzburg Muhammad Riyad, il bombarolo di Ansbach Mohamed Daleel, pur nella loro documentata psicopatia, sono entrati in contatto con lo Stato Islamico. Direttamente, o indirettamente. Hanno comunicato nel segreto con chi ha fornito istruzioni, consigli, una ragione per farlo. Hanno sfruttato la cyber-jihad nel suo potenziale massimo: la rete di comunicazioni criptate invisibili all'intelligence.

Le darknet, Tor, le Virtual private network (Vpn), Telegram, le mail cifrate con doppia password, i software che ingannano il gps del telefonino e ti posizionano in un posto dove non sei, la app per bambini ("Alphabet") che insegna ad associare ogni lettera dell'alfabeto a un oggetto, un fucile d'assalto o un tipo di bomba in questo caso. I mezzi sono tanti e i jihadisti non sono muti. Parlano, ma dietro scudi digitali. Hanno inzeppato la loro cassetta degli attrezzi di tecnologia di ultima generazione e a basso costo.

La media house "As-Sahab" con cui Al Qaeda fabbricava e diffondeva nel 2001 rudimentali messaggi in Pakistan e Afganistan è archeologia. Adesso è un altro mondo, molto più complesso.

Adesso c'è Opera. Opera è uno dei browser per navigare in anonimato su Internet. È compatibile con il sistema android per telefonini, che a quanto pare è il più usato dagli islamisti. Con Opera gli aspiranti jihadisti scaricano i manuali per fabbricare ordigni con fertilizzante, chiodi, bulloni e poco altro. Nell'aprile 2019 gli analisti di "Flashpoint", società che fornisce strumenti di intelligence per frugare nelle profondità del Deep Web, scoprono un forum di fanatici religiosi dove vengono condivise informazioni sull'uso di Opera e di Tor. Con accortezze che dimostrano, se ancora ce ne fosse bisogno, il grado di expertise di cui si sono dotati i cyberjihadisti di Al Bagdhadi: "*Scaricate il software di Tor su una pennetta usb, utilizzatelo solo negli internet café: mai due volte nello stesso posto, mai due volte sullo stesso computer*". E sulle Vpn, le reti di telecomunicazione private, segnalano: "*Non sono del tutto sicure, lasciano una traccia del numero seriale dell'hard disk da cui si può risalire a noi*".

Intercettando i telefoni alla maniera tradizionale si rischia di perdere tempo, dunque. Raramente si ascoltano commenti sullo Stato Islamico o su obiettivi sensibili da far saltare in aria. Per quello ci sono le chat criptate, Telegram e Whatsapp. L'ordine di colpire l'Italia giunto dalla Siria ad Abderrahim Moutaharrik, kickboxer marocchino di Lecco, era contenuto in un messaggio audio trasmesso su Whatsapp. I poliziotti della Digos e i carabinieri del Ros, che arrestarono Moutaharrik

nell'aprile 2016 con l'accusa di terrorismo, lo captano solo grazie a una cimice piazzata nella sua auto.

Osserva una fonte qualificata dei nostri servizi segreti interni: "L'utilizzo massiccio di tecnologia per cifrare le conversazioni è un ostacolo serio. Dobbiamo scoprire un potenziale kamikaze dal comportamento che assume. Una volta individuato, allora, solo allora, lo monitoriamo con microspie e virus digitali".[6]

In Siria, nei ranghi dello Stato Islamico, esiste una piattaforma che ha un compito speciale: rendere trasparenti le direttive che Abu Muhammad Al Adnani, la mente della campagna del terrore in Occidente, invia alle cellule in Europa.

Si chiama "*United CyberCaliphate*", il CyberCaliffato Unito. Si occupa pure di tenere aggiornata la grande rete di comunicazioni occulte dell'Isis. Sono canali che qualche falla, tuttavia, ce l'hanno.

Sulle darknet sono da sempre infilitrati centinaia di agenti di polizia. Un segreto di Pulcinella svelato da Edward Snowden nel 2012: con documenti top secret ha dimostrato che la Nsa, la maggiore agenzia di spionaggio degli Stati Uniti, è in grado di "rastrellare" il traffico su Tor. È il motivo per cui il governo americano non vuole "accecare" questi canali e i social network su cui girano i contenuti di propaganda jihadista. Contano sulla capacità dei loro 007 di "sniffare" qualsiasi brandello di informazione. Però, dopo la strage di Dacca (29 morti, tra cui 9 italiani), l'Europa spinge per isolare il più possibile le reti del'Isis, per evitare di renderle cassa di risonanza dei video delle esecuzioni. Nessuno ha ancora trovato il modo di farlo. Ma intanto il lupo solitario è diventato meno solo.

6 https://www.repubblica.it/esteri/2016/07/26/news/terrorismo_rete_criptata_stato_islamico_cyber_jihad-144816976/

LE NUOVE ARMI DI MASSA

Secondo alcune stime del Market Info Group L.L.C., nel decennio 2014/2024, il mercato mondiale delle cosiddette *cyber weapons* supererà i 3.000 miliardi di euro.

Le cause di tale fenomeno sono molteplici:

- numero crescente delle minacce alle infrastrutture e alle industrie critiche; aumento delle spese per la difesa
- aumento delle iniziative aziendali
- crescita della preferenza da parte dei governi delle armi cibernetiche negli scontri bellici

I paesi all'avanguardia in questo settore sono sicuramente Stati Uniti, Cina, Russia, Corea del Nord, Corea del Sud e Iran.

Dei paesi appena citati, la Cina pare sia quello che si svilupperà di più in quanto, dati alla mano, gli utenti sono 400 milioni, 1/3 della popolazione mondiale, con un aumento di 50 milioni all'anno rispetto ai 250 milioni americani. Se saliamo di livello, ovvero quello globale, su una popolazione stimata nel 2020 di 7.5 miliardi, si ipotizza che gli utenti di internet saranno 4,8 miliardi.

Grazie a questi dati, è facile intuire che in futuro ci sarà un nuovo e grande tipo di conflitto, ovvero su chi deciderà le regole del cyberspazio, avendo in mano la rete e quindi il "mondo". Quindi, si farà sempre più ricorso alle armi cibernetiche, perché meno costose rispetto a quelle cinetiche. Infatti, basti pensare che un caccia costa tra gli 80 e i 120 milioni di dollari, mentre si valuta che un'arma cibernetica parte dai 300 fino ai 50 mila dollari. Inoltre, questo non è l'unico vantaggio: esse sono più precise, efficaci, lanciabili da qualunque parte del mondo, per lo più anonime e personalizzabili (*tailored of the target*). Tuttavia, esse possono essere definite "one-shot", perché quando vengono rivelate non possono più essere utilizzate, dato che non porterebbero allo stesso effetto sorpresa della prima volta, vanificando o indebolendo così l'attacco. Questo tipo di armi offensive sono di tre tipi: semplici, moderatamente complesse e complesse.

Nel primo caso si sfrutta la mancanza di autenticazione, nel secondo si individua il processo di controllo e nel terzo viene alterato il processo in modo che il bersaglio non si accorga del pericolo.

Tuttavia, non tutte le strutture sono collegate ad internet, per questo si usano altri strumenti per intaccarle come la chiavetta USB. Un esempio è certamente il caso Sunxet, che vide coinvolta una centrale nucleare in Iran.

Per quanto riguarda le cyber weapons difensive, esse sono più costose. Se invece volessimo dare una definizione di arma cibernetica, cominciamo con il dire che non ve n'è ancora una accettata a livello internazionale. Una definizione molto elementare è quella di Umberto Gori, riportata nel 2014 su Cyber Warfare: "*uno strumento informatico costituisce una cyber weapons se, e soltanto se, ha una valenza almeno potenzialmente letale, e cioè distruttiva di cose o persone*". Secondo la definizione di Stefano Mele, si tratta invece di "*un'apparecchiatura, un dispositivo, ovvero qualsiasi insieme di istruzioni informatiche dirette a danneggiare illecitamente un sistema informatico o telematico avente carattere di infrastruttura critica, le sue informazioni, i suoi dati o i suoi programmi, in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione totale o parziale, o l'alterazione del suo funzionamento*".

Dunque, come già affermato, il fatto che non ci sia una definizione concordata a livello internazionale non permette di stabilire un quadro giuridico capace di valutare in maniera oggettiva la gravità della minaccia e la responsabilità di chi ha commesso il fatto, lasciando così allo stato ampia discrezionalità al riguardo. Un tentativo, però, è stato fatto con il *Tallin Manual on the International Law Applicable to Warfare*, scritto da un gruppo indipendente di esperti, che individua tre principi importanti: riservatezza, integrità e disponibilità.

In ordine di pericolosità riconosciamo:

- Attacchi Denial of Service (Dos) e vandalismo web, in cui lo scopo è di sovraccaricare i siti internet. Questo attacco mira a mettere fuori uso temporaneamente i sistemi colpiti, senza avere conseguenze di lungo termine.

- Attività di raccolta di dati sensibili, ci si impadronisce di password, documenti, progetti. Da qui parte l'attività di spionaggio che può portare anche alla cancellazione dei dati del nemico che dovrà poi riscrivere tutto.

- Attacco alle apparecchiature, dove si mira a distruggere le apparecchiature militari, i satelliti e i sistemi di comunicazione.

- Attacchi diretti alle infrastrutture, andando a colpire quelle strutture che erogano servizi essenziali come energia, acqua ecc. Sulla base di questi attacchi, un sistema di difesa all'altezza dovrebbe essere basato su:

- controllo delle reti;
- rivelazione e classificazione dell’attacco;
- decisione di appropriate contromisure

BITCOIN E CYBER TERRORISMO

Fino a poco tempo fa, prima del boom che lo ha caratterizzato negli ultimi anni, la più celebre delle criptovalute, ossia il Bitcoin, era conosciuta quasi esclusivamente per il suo utilizzo non propriamente ortodosso, ovvero come il mezzo di pagamento preferito dai criminali, cyber o meno che fossero, di tutto il mondo.

In particolare per quanto riguarda il saldo del riscatto dei tanto temuti cryptolocker. Tanto che, meno di un anno fa, *Digital4Trade* interrogò la giurista Anna Italiano[7] per comprendere se i fornitori di Bitcoin potessero essere considerati in qualche modo corresponsabili degli attacchi ransomware (per chi lo volesse sapere la risposta è negativa).

In questi mesi molte cose sono cambiate: innanzitutto, come accennato la crescita continua del valore della criptovaluta, sostanzialmente decuplicato nel giro di pochi mesi.

Inoltre, il Bitcoin è uscito dai circuiti del Deep Web per affermarsi sempre di più come una vera e propria valuta utilizzata anche per gli scambi "legali", come dimostra la nascita di sportelli bancomat dedicati e addirittura di *futures* sui Bitcoin, a testimonianza di una crescente attenzione dei circuiti finanziari tradizionali.

D'altra parte, però, non v'è dubbio che il legame Bitcoin-Deeep Web continui a rimanere saldo: l'anonimato richiesto dagli amanti del Deeep Web, è facile da capire e si sposa benissimo con le caratteristiche stesse di Bitcoin e della Blockchain. Innanzitutto i pagamenti non passano tramite circuiti controllati dalle istituzioni come quelli tradizionali bancari, rendendo così possibili transazioni da un capo all'altro del mondo. Senza necessità di esporre la propria identità e, dunque, tutelando ai massimi livelli la privacy. Non solo: il sistema di validazione delle transazioni concepito dalla *blockchain*, basato sull'attività dei *miners*, rende possibile assicurare la sicurezza dell'avvenuta transazione, senza lasciare spazio al dubbio.

Altro aspetto considerevole di Bitcoin è legato all'abbattimento dei costi di transazione: la maggior parte delle operazioni può essere gestita senza alcuna commissione, a differenza di quanto accade con gli intermediari finanziari. Gli utenti, però, sono incoraggiati a pagare una piccola commissione volontaria in cambio di una 'maggiore velocità di conferma' della transazione e per ricompensare i "minatori". Un altro punto importante a favore del rapporto Bitcoin-Deep web è la velocità: in realtà la validazione delle transazioni in Bitcoin non è di per sè particolarmente rapida

7https://www.blockchain4innovation.it/bitcoin/blockchain-non-ce-favoreggiamento-cryptolocker-bitcoin-strumento-legale/

(ed è anzi uno degli aspetti su cui la comunità sta cercando di migliorare), ma lo è nettamente di più rispetto ai classici bonifici internazionali, che possono impiegare anche giorni.

Insomma, come riassume il documento dell'Agid[8] - "*Le caratteristiche che rendono le criptovalute utilizzabili nell'ambito della frode, del terrorismo, del riciclaggio di denaro sporco e del crimine organizzato, designano una delle maggiori sfide per le forze dell'ordine, le autorità di regolazione e i governi nazionali. L'ambizione di dar luogo a trasferimenti di denaro veloci, sicuri e con costi di transazione minori rispetto all'attuale fiat money in tutto il mondo porta con sé il rischio di facilitare e offuscare transazioni legate ad attività criminali, incluso il riciclaggio di denaro e il finanziamento al terrorismo, il commercio di droghe e la frode su scala globale. Tale pericolo va affrontato e combattuto con regolamenti e leggi ad hoc, al fine di sfruttare i vantaggi della tecnologia blockchain*".

A quanto pare, però, la crescente popolarità di Bitcoin ha provocato alcune ripercussioni nei mercati del dark web. Secondo quanto si può leggere su svariati forum, le spese di trasferimento per accelerare la velocità di transazione in questi ultimi mesi sono diventate molto più alte.

Questo sta spingendo molti utenti del Deep Web a scegliere le Altcoin.[9]

RESPONSABILITÁ DEL PROVIDER

Se da un lato abbiamo che uno dei problemi maggiori è l'identificazione del terrorista online, dall'altro cè quello dell'individuazione del giudice nazionale competente in una realtà, quella di internet, che sostanzialmente non conosce confini territoriali, figurarsi i confini giuridici.

Uno degli aspetti più discussi riguarda, infatti, la responsabilità dell'ISP.

Con Internet Service Provider, chiamato anche ISP o Provider, viene definito come quel soggetto che esercita un'attività imprenditoriale che fornisce agli utenti dei servizi come la connessione, la posta elettronica, lo spazio per la memorizzazione di siti web o blog o creazione degli stessi, le chat line e host di motori di ricerca.

Si può far riferimento anche all'Access Provider, il cui compito è per lo più quello di accertare l'identità dell'utente che richiede il servizio, di acquisirne i dati anagrafici, e, quindi, di trasmettere la richiesta all'Autorithy Italiana affinché provveda all'apertura del relativo sito web. L'Access

8 Agenzia Governativa per l'Italia Digitale

9 Alternativa al Bitcoin ma ancora più difficile da criptare

Provider può anche limitarsi a concedere al cliente uno spazio, da gestire autonomamente sul disco fisso del proprio elaboratore.

Attualmente seppur con formule non pienamente sovrapponibili, il legislatore ha escluso la rilevanza penale dei servizi offerti dall'ISP alla realizzazione del fatto tipico qualora non siano almeno accompagnati, al momento della trasmissione o della memorizzazione dei dati, da una effettiva conoscenza del contenuto illecito degli stessi, ovvero il provider era all'oscuro del contenuto trasmesso dall'utente che usufruisce del servizio.

Nei primi anni 2000 le piattaforme del web dovevano essere neutrali nei confronti dei contenuti veicolati, e la direttiva e-commerce, prevedendo un'esenzione da responsabilità per contenuti immessi da terzi, ha consentito la crescita e la moltiplicazione dei servizi online, in particolare quelli che permettono la diffusione di contenuti generati dagli utenti.

Oggi, invece, si richiede un sempre maggiore intervento regolamentare da parte dei provider sui contenuti immessi da terzi.

Il G7 di Taormina (maggio 2017) è stato il primo momento di vicinanza tra i Governi Europei e i maggiori provider delle comunicazioni tradizionali e web per avviare un memorandum d'intesa.

Il 12 settembre 2018, la Commissione Europea presentava la proposta di regolamento sulla prevenzione della diffusione di contenuti terroristici online[10]. Il progetto legislativo mira ad introdurre nell'ambito dell'Unione Europea l'obbligo di imporre agli "hosting service provider" un'azione preventiva contro i contenuti terroristici.

Il regolamento si aggiunge alla direttiva sul terrorismo (Directive 2017/541) che da settembre 2018 è attuabile. La direttiva comprende misure per contrastare i contenuti online compresa la "pubblica provocazione" alla commissione di reati di terrorismo, adottando anche misure di blocco e rimozione di tali contenuti. Il regolamento estende tali misure al materiale di reclutamento o formazione di terroristi.

Il nuovo regolamento si inquadra in una lunga serie di iniziative dell'Unione europea volte a regolamentare e limitare i contenuti online, sia illeciti che leciti, anche con misure di *soft law*.

In tale direzione, infatti, abbiamo avuto già una raccomandazione (non vincolante) per il contrasto ai contenuti illegali online, la direttiva *Audio Visual Media Service*, l'accordo tra le principali aziende del web per il contrasto all'*hate speech* e, ovviamente, la stessa direttiva sul copyright.

10 https://www.ilgiornale.it/news/mondo/lisis-festeggia-covid-19-punizione-allah-1842647.html

Il progressivo passaggio da accordi non vincolanti a regolamentazioni legislative indica l'intensificarsi dell'azione della Commissione Europea, caratterizzata da un progressivo inasprimento dei requisiti per gli intermediari della comunicazione online.

I redattori della newsletter *Al Naba*, organo di informazione interna dell'Isis, vantano la fortuna di avere tutto chiaro. Il coronavirus "*è un tormento che Dio può mandare contro chi vuole, e Lui ne ha fatto una benedizione per i credenti. Chiunque stia sulla terra, aspettando che la piaga colpisca, e sapendo che colpirà solo coloro che Dio ha scelto, per lui sarà come la ricompensa di un martire*".[11]

La prova migliore della volontà divina è nell'attuale distribuzione del morbo.

La malattia, sottolineano i fondamentalisti dello Stato Islamico, "*ha colpito (ne sia lode al Signore) soprattutto le Nazioni idolatre*". Il riferimento non è solo ai Paesi occidentali ma anche all'Iran, centro focale dell'Islam sciita e dunque nemico odiatissimo degli estremisti sunniti. Nell'editoriale di Al Naba sul virus non c'è spazio per la compassione: "Possa Dio aumentare la sofferenza degli infedeli e tenere al sicuro i credenti".

A guardare l'impaginazione della newsletter, un brivido è inevitabile, perché per illustrare la pagina con l'editoriale sul tema, i jihadisti hanno utilizzato una foto di soldati italiani con la mascherina, impegnati nel controllo a un posto di blocco.

Il problema, però, è che il virus non sembra seguire i desideri dei fondamentalisti: nei giorni scorsi il blog *Difesa&Sicurezza* ha segnalato un'epidemia nella zona di Deir Ezzor[12], dove ancora cellule dell'Isis affrontano le milizie filo-iraniane. I contagiati sarebbero forse 150, con poche o nulle possibilità di terapia. Anche perché, alla luce della dottrina integralista, per un jihadista ammettere di aver preso il virus sarebbe come confessare di non essere un buon credente.

Infatti, da lì a poco si registra il passo indietro anche dell'Isis di fronte alla pandemia da Covid-19.

Nell'ultimo numero della rivista jihadista online Al-Naba, lo Stato islamico raccomanda ai suoi militanti di stare lontano dalle terre dell'epidemia, cioè l'Europa, per il rischio di rimanere infetti. In pratica gli attacchi vengono rimandati a quando l'emergenza sanitaria sarà finita. I terroristi hanno anche diramato "*indicazioni in base alla sharia*" per contrastare il diffondersi del Covid-19 nei loro ranghi, corredate da citazioni coraniche.

Sono indicazioni in linea con quelle dei governi occidentali. La rivista invita a "coprirsi bocca e naso quando si starnutisce o tossisce" per non infettare gli altri, a lavarsi le mani "regolarmente", a

11

12 https://www.difesaesicurezza.com/difesa/iraq-siria-probabile-epidemia-di-coronavirus-tra-isis-e-i-miliziani-pro-iran/

usare dispositivi di protezione per il volto quando si esce e soprattutto a “limitare gli spostamenti non necessari”, cioè a restarsene a casa come i comuni cittadini.

Ma tra le direttive date dall’Isis c’è anche quella di “affidarsi ad Allah e cercare protezione in lui” e a “porre la fiducia in Dio”.[13]

13 https://www.lastampa.it/esteri/2020/03/15/news/il-coronavirus-ferma-anche-l-isis-stop-agli-attacchi-in-europa-1.38595717

CONCLUSIONI

Il fenomeno terroristico in tutte le sue manifestazioni rappresenta una sfida tanto insidiosa quanto affasciante per le organizzazioni governative e tutti quei soggetti che non raccolgono il messaggio della lotta al nemico di sempre attraverso qualsiasi mezzo.

Nel nostro ordinamento la norma nella lotta al terrorismo è sinora quella dell'articolo 270 bis, rubricato appunto "*associazioni con finalità di terrorismo anche internazionale*", al quale, a partire dal 2005, sono state affiancate fattispecie di tipo mono soggettivo per cercare di contenere la progressiva evoluzione del fenomeno terroristico.

La creazione di nuovi strumenti giuridici secondo le peculiarità della rete, di un diritto penale propriamente informatico, pare la soluzione migliore, dato che le fattispecie informatiche e internet difficilmente si adattano agli istituti tradizionali esistenti, se non con forzature e compromettendone spesso la natura.

La conseguenza è che la migliore risposta all'abuso di apertura della rete è di concedere ancora più apertura, sia dal punto di vista delle tecnologie utilizzabili, sia dal punto di vista della regolamentazione futura. Infatti, una regolamentazione di internet troppo vincolante negli stati democratici attuali può minacciare lo sviluppo di democrazie emergenti. Le attività terroristiche non possono danneggiare più di tanto internet, ma un'attività legislativa troppo vivace e stringente, anche se emanata in risposta ad atti di terrorismo, lo può fare.

Per far ciò è necessario un maggior coinvolgimento dei soggetti privati, quali internet service provider, accanto all'autorità pubblica, nella definizione delle modalità di regolamentazione della rete. In questo modo il legislatore mantiene il controllo della regolamentazione della rete, beneficiando del supporto di quei soggetti privati che hanno una maggiore conoscenza della rete e dei fenomeni informatici.

Inoltre è possibile beneficiare dell'aiuto degli utenti tradizionali; una maggiore responsabilizzazione di tali soggetti nella segnalazione all'autorità competente dei contenuti a matrice terroristica, quali files propagandistici o video di attentati. La segnalazione di tali contenuti, e non la condivisione, aiuta a contenere gli effetti di tali messaggi, quali quello di generare un clima di panico e terrore nella popolazione, e di limitare la capacità diffusiva, e in questo caso distorta e non garantita, di internet.

Un sistema piegato alle esigenze emergenziali del periodo e disposto a sacrificare diritti fondamentali individuali, come la privacy, potrebbe generare risvolti pericolosi.

Infine, secondo i dati raccolti è più facile bloccare la propaganda cyber-terrorista direttamente sul web o sulle app-mobile, con il massimo e innegato supporto dei vari soggetti proprietari di service provider, rispetto sicuramente al più alto costo nel dover ricercare tali individui nel deep web o nel darknet.

BIBLIOGRAFIA & SITOGRAFIA

(i) Giovanni Miragliotta, Alessandro Perego, Marco Taisch; Industria 4.0, che cosa succede in Europa e negli Usa, 2016

(ii) A. BALSAMO, Decreto antiterrorismo e riforma del sistema delle misure di prevenzione, Diritto Penale Contemporaneo, 2015

(iii) A. CIPRIANI, G. CIPRIANI, La nuova guerra mondiale. Terrorismo e intelligence nei conflitti globali, Sperling & Kupfer Editore, 2005

(iv) A. TENCATI, Codici penali militari e ordinamento militare, LA TRIBUNA EDITORE, 2016

(v) D. ALBANESE, Partecipazione all'associazione con finalità di terrorismo 'stato islamico': una pronuncia di condanna della corte d'assise di milano, Diritto Penale Contemporaneo, 2016

(vi) D. E. DENNING, Cyberterrorism, George Town University, 2000

(vii) G. WEIMANN, How modern terrorism uses the Internet, Report dello United States Institute of Peace, 2004

(viii) M. M. PETRONE, Internet e le sue insicurezze, strumenti, soggetti e contesti, GIAPETO Editore, 2014

(ix) Presidenza del Consiglio dei Ministri, Relazione sulla politica dell'informazione per la sicurezza, 2019

(x) R. SPREAFICO, La responsabilita' del provider e del fornitore di servizi telematici dopo il d. lgs. 70/2003

(xi) United Nation Office on Drugs and Crime (UNODC), the use of the internet for terrorist purpose, Organizzazione delle Nazioni Unite, ONU

SITOGRAFIA

(xii) https://www.yumpu.com/it/document/read/55712064/terrorismo/3

(xiii) https://www.techcompany360.it/tech-lab/altcoin-cosa-sono-e-come-funzionano-le-criptovalute-sorelle-di-bitcoin/

(xiv) *https://www.repubblica.it/esteri/2016/07/26/news/terrorismo_rete_criptata_stato_islamico_cyber_jihad-144816976/*