Poliziamoderna

# La minaccia corre sul Web

L’eco dei colpi di kalashnikov esplosi a Parigi lo scorso 7 gennaio contro la redazione di Charlie Hebdo è risuonata per tutto l’Occidente gettando nuova luce su quelle immagini di esecuzioni e di attentati che rimbalzavano dalle nostre televisioni, ma che provenivano da Paesi lontani. Forse troppo lontani per poter sentire il rumore degli spari e delle bombe. Pensavamo forse di essere al sicuro dal terrore jihadista e invece sangue e paura sono stati versati a piene mani nel cuore del Vecchio Continente: di colpo tutti hanno compreso la gravità della minaccia terroristica, cresciuta giorno dopo giorno a partire da quel 29 giugno 2014, prima notte del mese di Ramadan, con la proclamazione del Califfato dell’Isis, in seguito autodefinitosi Is (Islamic state). Una sensazione crescente di allarme favorita anche dalla costante e rapida evoluzione tecnologica dei sistemi e dei servizi di comunicazione elettronica: la loro inarrestabile diffusione ha infatti messo a disposizione degli utenti della Rete una sempre maggiore quantità di informazioni eterogenee difficili da controllare e, eventualmente, da bloccare. Ed è in questo scenario che l’Is ha saputo muoversi con sorprendente abilità, dando vita a una guerra santadel tutto inedita, in cui a un esercito capace di compiere atti di pura barbarie si è affiancato l’uso spregiudicato e martellante delle più sofisticate tecnologie comunicative. Sugli schermi delle tv di tutto il mondo, e attraverso la Rete mediante l’utilizzo di pc o smartphone, vengono diffusi, senza risparmiare neppure i particolari più raccapriccianti, video di decapitazioni, esecuzioni di massa e incitazioni a uccidere ogni oppositore, anche se musulmano. Nell’ultimo decennio, il jihad è mutato drasticamente e, attualmente, ha assunto una nuova forma, meno regionale e gerarchizzata, meno organizzata, ma molto più pericolosa, capace di colpire ovunque e in ogni momento. Il mondo virtuale ha semplificato questa rivoluzione, permettendo agli jihadisti di divulgare oltre i confini del Medio Oriente il proprio credo salafitico-jihadista radicale che giustifica il dogma antisemita, l’animosità, l’odio e la violenza contro il mondo occidentale. Internet è il mezzo di comunicazione scelto per mettere in contatto gli aspiranti jihadisti tra loro e con le filiere internazionali; inoltre la Rete è fonte illimitata di informazioni e di istruzioni utili per la costruzione e l’utilizzo di armi e ordigni anche non convenzionali. Il Web è lo spazio dove il terrorismo “molecolare” si incontra e si radicalizza. Terrorismo molecolare di matrice Al Qaeda o di matrice Al Baghdadi , per il quale il sottosegretario delegato all’intelligence Marco Minniti ha più volte denunciato i rischi di fronte al Parlamento, è quello che ci troviamo a fronteggiare in Europa: cellule forse coordinate , ma sicuramente chiuse e autonome che, come detto, possono colpire ovunque. Ciascuna cellula agisce per conto proprio e non prende direttive da nessuno. Alcuni agiscono come singoli e per tanto si parla di “lupi solitari”. Proprio per quanto concerne il ruolo del Web, nelle strategie dei gruppi riconducibili al fondamentalismo islamico è emerso la piena consapevolezza che per assicurare la divulgazione delle proprie ideologie e il reclutamento dei militanti, anche dei foreign fighters e finanziatori, è necessaria la costante presenza attiva nello spazio cibernetico. Un salto di “qualità” comunicativa messa in atto soprattutto dall’ IS, che proprio per questo si avvale di propri siti web per la divulgazione di video riguardanti operazioni jihadiste oppure contenenti dichiarazioni politiche e “fatwa” (pareri e indicazioni) religiose. Non manca poi la messa on line di pubblicazioni periodiche (vedi box), di interviste e di messaggi da parte di scrittori vicini al mondo jihadista sull’utilizzo dei moderni strumenti di comunicazione elettronica ai fini del jihad: interventi che diventano ben presto oggetto di discussione nei forum, nei blog, sui social network e su altri canali di comunicazione.

**Le attività investigative** Di fronte a questo scenario in continua evoluzione e sempre più polverizzato, il Servizio polizia postale e delle comunicazioni impegna oggi buona parte delle proprie energie in una attività di costante monitoraggio della Rete, i cui primi passi risalgono al 2007 in collaborazione con le forze di polizia specializzate di altri Paesi europei e degli Stati Uniti. Questa specifica conoscenza, maturata nel corso degli anni, ha fatto sì che la polizia postale italiana sia oggi in prima linea nell’evidenziare e nell’analizzare i diversi sistemi adottati dai gruppi militanti che utilizzano Internet per perseguire il “Al-Jihad Al-I’lami”, ovvero il “jihad mediatico”. La tattica seguita dai militanti jihadisti è quella di condurre una “guerra di percezione”, dove la politica e la propaganda occupano il primo posto, utilizzando il potere della tecnologia e di Internet per minare l’autorevolezza dei governi occidentali e per convincere gli utenti della Rete ad unirsi alla jihad. E’ però da tenere presente che sulla Rete il terrorismo è un fenomeno molto dinamico, all’interno del quale i siti web mutano costantemente, appaiono all’improvviso e, di frequente, si trasformano per poi sparire rapidamente e riapparire ancora, con una url diversa o attraverso una diversa allocazione. Questa attività di glorificazione del jihad avviene utilizzando diverse forme multimediali di diffusione, prima fra tutte l’hacking “jihad elettronico”, vera e propria guerra digitale con la quale gruppi organizzati compiono azioni di pirateria informatica perpetrando attacchi informatici ai siti web di aziende o istituzioni considerati nemici dei jihadisti. Altre forma di propaganda è quella delle pubblicazioni on line. Internet

è infatti lo strumento utilizzato per creare e condividere forum di discussione, blog, video youtube, gruppi sui social network (Twitter e Facebook) con contenuti che vanno dall'incitamento al jihad e alle sue virtù alla difesa dei mujaheddin e del loro onore da chiunque intenda colpirli, dall'emersione della coscienza ideologica del jihad al sostegno intellettuale e dallo studio della legge islamica, fino al controllo degli oppositori del jihad e loro esposizione al disonore. Il controllo di questa ingente quantità di informazioni che ogni giorno viaggia in Rete è resa ancora più difficile dal fatto che l'accesso a molti siti è condizionato da password e dalla georeferenziazione degli IP address di accesso ovvero dalla preventiva presentazione da parte di iscritti/militanti. Numerosa è poi la produzione di testi rintracciabili nel Web, da quelli religiosi alle trascrizioni dei saggi, dai comunicati ai discorsi e dichiarazioni dei loro leader, ai testi sulla sicurezza personale e su come eludere la sorveglianza del nemico, solo per indicarne alcuni. Un capitolo a parte meritano i video postati in Rete che sono essenzialmente di tre tipi: quelli che mostrano e rivendicano attentati ed esecuzioni, contribuendo alla causa jihadista attraverso la dimostrazione del proprio coraggio, determinazione e dedizione per sconfiggere il nemico, e che hanno soprattutto un grande potere di attrazione di nuove reclute e finanziatori; video di addestramento virtuale, utilizzati per l'esercitazione ad azioni di guerriglia e che forniscono, gradualmente, istruzioni sull'impiego di armamento leggero e per la costruzione di ordigni esplosivi improvvisati; video dei discorsi e dei comunicati dei leader jihadisti ma anche videogame e musica rap. Oggi il costante monitoraggio della Rete effettuato dalla Postale, anche a seguito di specifiche segnalazioni della Polizia di Prevenzione e del Comparto intelligence (che svolgono le attività investigative sul campo e con i quali si è in continuo scambio informativo) è focalizzato su forum, siti, blog e profili o gruppi di social network, cui il numero è in continuo cambiamento vista la volatilità degli stessi. Un'apposita task force composta da 20 operatori lavora h/24 per individuare processi di consolidamento e aggravamento di posizioni tendenti all'estremizzazione di tematiche di ispirazione religiosa islamista. In tale ottica l'indicazione di massima è quella di evitare interventi e provvedimenti dell' autorità giudiziaria, preferendo invece di continuare a seguirne l'evoluzione per non disperdere preziosi spunti di approfondimento. Laddove, invece, lo spazio monitorato viene ritenuto dagli operatori di immediato interesse investigativo, si intraprendono le iniziative necessarie alla rimozione o al sequestro dei suoi contenuti, anche se, trattandosi nella quasi totalità dei casi di siti sedenti in Stati esteri, la possibilità di oscurarne i contenuti è legata alla collaborazione del singolo Paese che, in forza di una rogatoria internazionale proposta dall'a.g. italiana, procederà alle operazioni di oscuramento o rimozione dei contenuti del sito, mentre, sempre con una disposizione dell'a.g., è possibile inibire l'accesso ai siti citati a tutti gli utenti che si collegano dal territorio italiano. Per dare un'idea della mole di lavoro svolto dalla Postale, basti pensare che in questi ultimi due mesi gli spazi virtuali monitorati sono stati circa 400. Quando il monitoraggio fa rilevare la necessità di procedere a ulteriori approfondimenti investigativi al di fuori dei confini nazionali, si segue un modus operandi ormai consolidato che prevede la attivazione di canali internazionali di cooperazione di polizia, finalizzata alla valutazione della minaccia e alla identificazione dell'origine di essa. Il raccordo operativo con i tradizionali canali di cooperazione di polizia, Interpol ed Europol è reciproco e costante e, in ragione dell'assoluta urgenza imposta dalla serietà della minaccia, nell'emergenza si tende a ricorrere al "punto di contatto 24/7 HTC Emergency" previsto dalla Convenzione di Budapest. La collaborazione con gli Stati europei e con gli USA fa sì che lo scambio di informazioni venga arricchito in tempo reale direttamente con il collaterale organo di polizia estero. Europol, infine, contribuisce sul piano strategico attraverso un progetto che permette di condividere a livello internazionale una banca dati nella quale ciascun Paese aderente inserisce l'esito delle proprie attività di monitoraggio della Rete, allo scopo di creare una sorta di archivio documentale condiviso di documenti inerenti l'area integralista islamica. In questo contesto complesso e complicato da interpretare, tra gli ostacoli principali all'attività di monitoraggio della task force della Polizia delle comunicazioni ci sono la necessità di una perfetta conoscenza della lingua araba, utilizzata per le quasi totalità delle comunicazioni da jihadisti ed aspiranti tali, e la piena padronanza di schemi culturali assolutamente diversi, come quelli che caratterizzano la religione islamica e i suoi gruppi più estremisti. Il primo problema è stato risolto facendo ricorso a interpreti madrelingua, il secondo attingendo a mediatori culturali ed esperti in storia e cultura araba. I dialetti però variano da regione a regione, da cellula a cellula e minime sfumature di suoni e di scrittura danno vita a mille significati diversi per uno stesso vocabolo. Anche se le deliranti parole lanciate nel Web sono ormai sopravanzate dalla follia dei gesti.

**primo dirigente del Servizio polizia postale e delle comunicazioni*

_____ ***Giro di vite*** Lo schema di decreto legge recante "misure urgenti per il contrasto del terrorismo, anche di matrice internazionale" in discussione in questi giorni, e predisposto nell'intento di rafforzare e aggiornare gli strumenti normativi previsti dal nostro ordinamento per il contrasto del terrorismo, prevede, in particolare, l'introduzione di specifici strumenti volti a contrastare l'utilizzo del Web da parte di gruppi e organizzazioni terroristiche a fini di proselitismo e addestramento di nuovi adepti. In particolare, l'articolo due del decreto, completa il pacchetto di interventi volti a contrastare il fenomeno dei foreign fighters e le organizzazioni che compiono condotte con finalità di terrorismo di cui all'art. 270 sexies codice penale. Vengono introdotte a tal fine misure tese a contenere e reprimere le crescenti azioni poste in essere attraverso lo strumento telematico, idoneo a raggiungere un numero sempre maggiore di potenziali combattenti,

come emerso anche dalla recente attività investigativa sul fenomeno dei cosiddetti “lupi solitari”. Integrando quanto già previsto dall’art. 7 bis del decreto legge n. 144/2005 convertito dalla legge del 31 luglio 2005 – varato a seguito degli attentati terroristici di Londra – si perfezionano le misure di contrasto all’utilizzo delle reti telematiche per finalità di istigazione e di proselitismo posto in essere ricorrendo a internet, seguendo il modello già sperimentato per il contrasto della pornografia sul Web. In particolare con il comma 1 si prevede l’aumento della pena della reclusione per i reati di istigazione e apologia del terrorismo, (art. 302 e 414 comma 4, cp.) quando tali fatti sono commessi attraverso strumenti telematici e informatici, attesa la particolare insidia del ricorso a tali mezzi, che diventa un’arma in mano ai terroristi che la utilizzano per alimentare il clima di terrore e per reclutare nuovi “sostenitori”. Il comma 2 prevede l’istituzione e il costante aggiornamento di una black list dei siti internet – alimentata dalle segnalazioni dei competenti organi di polizia – utilizzati per le attività terroristiche comprese quelle di proselitismo, arruolamento dei forein fighters, di addestramento ad attività di terrorismo anche internazionale. Viene stabilito che la black list è aggiornata dal Servizio polizia postale del Dipartimento di pubblica sicurezza, quale organo del ministero dell’Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione. Il comma 3 prevede l’obbligo per i fornitori di connettività di inibire l’accesso ai siti individuati con provvedimento della autorità giudiziaria procedente, mentre al comma 4 viene introdotta la possibilità per il pm che procede di ordinare ai fornitori dei servizi di hosting o di altri connessi alla rete internet di rimuovere i contenuti riguardanti i predetti delitti. L’ordine deve essere adempiuto immediatamente e comunque nell’arco di 48 ore. In caso di inosservanza la ag dispone l’interdizione all’accesso al dominio Internet nelle forme e con le modalità del sequestro preventivo. Le norme previste ovviamente richiedono una revisione dell’art. 53 del d.leg. 196/2003 (codice della privacy) che disciplina i trattamenti dei dati personali effettuati dalle forze di polizia e da altri organi di pubblica sicurezza per finalità di polizia.

_____ ***La cybernauta della Postale*** *di Anacleto Flori*

Da settimane ormai, da quel sanguinoso 7 gennaio parigino, quello che prima per gli operatori del Servizio polizia postale e delle comunicazioni era solo un lavoro di grande attenzione, di colpo è diventato un vero e proprio allarme rosso: scandagliare il Web in ogni suo angolo remoto alla ricerca di siti, blog, forum, social network, video che inneggino al jihad. Ma che soprattutto costituiscano una seria minaccia per il nostro Paese e non solo. Da quel giorno, un’ apposita task force, in tutto una ventina di persone, si alterna giorno e notte davanti ai monitor dei pc per cogliere una frase, un segno, un indizio che possa mettere gli investigatori sulle tracce di una “molecola” o di un “lupo solitario” pronti a colpire. Una task force fatta di poliziotti speciali, veri e propri “maghi” delle piattaforme tecnologiche, come l’operatrice cybernauta, profonda conoscitrice della lingua e della cultura araba, che Poliziamoderna ha intervistato per farsi raccontare cosa significa lavorare dietro le quinte, svolgere un lavoro tanto vitale per la nostra sicurezza quanto oscuro: per loro niente ribalta delle cronache, niente nomi, niente gradi e soprattutto nessuna immagine. Un gruppo destinato a restare nell’ombra, alla ricerca di altre ombre, quelle del terrore. **Com’ è cambiato il tuo lavoro dopo l’attentato a Charlie Hebdo?** A parte il fatto che in pratica la mia vita si svolge davanti al pc e che siamo arrivati a monitorare qualcosa come 400 piattaforme elettroniche, uno dei riflessi immediati è stato l’aumento esponenziale dei contatti e delle comunicazioni con Interpol e Europol: è vero che parliamo di canali che già da anni erano ben oliati, ma in questi giorni il flusso delle informazioni non è mai stato così continuo e veloce. A volte basta alzare il telefono per scambiare un’informazione o comunicare un intervento da fare. Proprio in questi giorni attraverso Interpol, ad esempio, abbiamo avuto una serie di segnalazioni relative a Ask.fm, un social molto usato, perché rispetto agli altri garantisce l’anonimato degli utenti. **Che tipo di segnalazioni?** Interpol ci ha comunicato che diversi adolescenti di 14-15 anni postavano la presenza di ordigni in diverse città italiane, da Roma a Venezia da Milano a Reggio Calabria e Palermo. Quasi sicuramente si trattava di “ragazzate”, ma di questi tempi nessuna minaccia può essere trascurata e così attraverso il territorio, gli autori delle frasi sono stati rintracciati e convocati in questura assieme ai genitori. E questo è un fenomeno che si sta diffondendo non solo in Italia, ma anche in altri Paesi. **A proposito dei maggiori social network, con Facebook, Twitter e gli altri social com’è il livello della collaborazione?** Se per altre questioni come commenti diffamatori e altro c’è maggior tolleranza, in materia di terrorismo c’è una collaborazione piena e incondizionata. Da questo punto di vista tutti i maggiori social, in particolar modo Facebook, mostrano una grandissima attenzione e, attraverso una forma di controllo interno,la pagina in questione viene oscurata. Lo stesso avviene anche se la segnalazione arriva ai social direttamente da un privato cittadino. Quest’ultimo aspetto è forse una delle novità più positive: ogni giorno attraverso le pagine del “commissariato on line” riceviamo segnalazioni su siti, forum e video da parte dei nostri utenti. È il segno di grande attenzione e di presa di coscienza da parte della cittadinanza di fronte a una minaccia che non conosce più confini. **Qual è la maggiore criticità del vostro lavoro?** La difficoltà di tradurre correttamente i commenti postati nei divesi forum. Basti pensare che fino a oggi abbiamo oscurato una ventina di siti che avevano sede in ogni parte del mondo, anche negli Stati Uniti e in Russia. Due di questi erano perfino in lingua cinese. E’ vero che la maggior parte sono in lingua araba, ma la presenza di decine e decine di dialetti che variano da Paese a Paese, da città a città e perfino da “molecola” a “molecola” rende il lavoro di traduzione estremamente difficile. Spesso anch’io, che pure conosco bene l’arabo, ho bisogno di farmi aiutare da

un esperto traduttore madrelingua: basta un piccolo errore e si rischia di sottovalutare una minaccia o di indagare un innocente; perché una volta venuta alla luce una traccia da seguire, sarà compito della Digos svolgere le necessarie attività investigative, come nel caso dello studente turco Furkan Semih Dundar espulso dal nostro Paese nelle scorse settimane. E' un compito delicato e il peso della responsabilità a volte diventa difficile da sostenere. Hai sempre paura che qualcosa ti sfugga, e il pensiero ricorrente è che magari nel momento in cui ti stacchi dal computer per andare via, proprio là, nel deep web si sta materializzando una nuova minaccia.

01/02/2015