"Studi" è una collana editoriale destinata a ospitare valide dissertazioni e tesi di laurea. I volumi raccolgono i risultati di un intenso lavoro di ricerca sulle fonti, fondamentale per contestualizzare l'oggetto d'analisi e proporre in maniera logica e coerente la tesi dell'autore. I testi sono caratterizzati da un chiaro impianto metodologico e dalla presenza di apparati paratestuali e bibliografici.

Il progetto valorizza il lavoro di autori che si affacciano al mondo dell'accademia portando in dote il loro punto di vista, originale e sperimentale, potenzialmente utile a riempire un vuoto di conoscenza di una determinata disciplina, offrire una sintesi di un tema complesso, proporre uno spunto acuto e fuori dal canone o suggerire inattesi riferimenti bibliografici.

tab edizioni

PASQUALINA FLORIO

Terrorismo cibernetico e sicurezza nazionale

Potenziale metamorfosi della minaccia eversiva

prefazione di Federico Sergiani

STUDI

Indice

p. 9 Prefazione di Federico Sergiani
15 Introduzione

19 Capitolo 1
Il concetto di terrorismo cibernetico
1.1. Definizione di terrorismo cibernetico: l'evoluzione della ricerca dall'Internet of Content all'Internet of Things, 19
1.2. Quadro nazionale: ricognizione teorica in materia di terrorismo cibernetico, 30
1.3. Un esempio di categorizzazione, 40
1.4. Terrorist Activity Framework, 50

55 Capitolo 2
Caso studio. Il digital jihād
2.1. Transizione spaziale: il terrorismo di matrice jihadista nel mondo virtuale, 55
2.2. Brevi cenni sulle metodologie OSINT, SOCMINT e VIRTUAL HUMINT, 74
2.3. Analisi OSINT. Digital jihād: il caso dell'Islamic State, 84
2.4. Digital Jihād Activity Framework, 106

p. 109 Capitolo 3
Sicurezza nazionale
3.1. Le infrastrutture critiche nazionali, 109
3.2. Analysis of Competing Hypotheses (ACH): il digital jihād rappresenta una minaccia per le infrastrutture critiche italiane?, 123
3.3. Buone pratiche di prevenzione e contrasto, 133

145 Conclusioni
151 Bibliografia

Prefazione

Immaginare la minaccia. Il terrorismo islamico digitale

«L'immaginazione vi porterà in posti in cui mai avreste pensato di arrivare». Questa è una frase riadattata da una celebre asserzione di Carl Sagan, un visionario – prima di tutto – con cui amo terminare le mie lezioni sull'analisi di intelligence. Se le abilità psicologiche e quelle accademiche come operative costituiscono il background necessario per un bravo analista di intelligence, finalizzato ad ottenere analisi il più possibile unbiased, è l'immaginazione che deve guidare lo stesso verso orizzonti che mai avrebbe pensato di esplorare. Perché esattamente come questo processo lo vive l'analista, spesso addestrato, così lo fa la controparte. Che spesso è capace di elaborare un pensiero laterale proprio per questo molto più sviluppato di chi è preposto al controllo e alla prevenzione di fenomeni che solo più recentemente sono finiti sotto la lente di osservazione della sociologia della devianza e del mutamento sociale.

Lo studio della dottoressa Florio non colpisce solo per la completezza dei contenuti, la capillarità dell'analisi, l'aver abilmente coniugato metodologie della ricerca accademica con quelle operative, doti che sono richieste ad ogni studente, secondo le sue possibilità, per poter ottenere un titolo

accademico al quale, con il proprio lavoro, si candidano. Il lavoro della dottoressa Florio colpisce per la sagacia immaginativa con cui ha metodologicamente svolto un lavoro, pur alle prime armi vista la giovane età dell'autrice, in cui è stata capace di penetrare un ambito estremamente complesso non solo da una prospettiva relativa all'ambito specifico del suo studio, quello dell'utilizzo della rete da parte del terrorismo islamico, quanto – allo stesso tempo – il lavoro operativo di un'analista "consumato" che avrebbe tranquillamente potuto aver elaborato lo stesso studio in una centrale di analisi di un'agenzia di intelligence, di un'azienda, di un think tank.

Mi sono occupato di terrorismo islamico per molti anni, forse troppi, da molteplici prospettive. L'aspetto digitale del fenomeno era sempre relegato ad un ambito mai estremamente rilevante – sebbene considerato – perché ci si concentrava più sui modelli operativi o sugli aspetti culturali come motivazionali che spingevano terroristi islamici di ogni ordine e grado non solo a sposare la causa della jihād – così come chi li foraggiasse ed aiutasse lungo la via – ma soprattutto a commettere attacchi di varia natura su territori occidentali o confondersi e appropriarsi, un tema che si rivelò presto di interesse, di tattiche più tipiche del crimine organizzato o di quello contiguo ad esso. Ma si sa, il diavolo è nei dettagli, e il lavoro della dottoressa Florio dimostra che proprio in una più generale coincidenza con l'appropriazione di tattiche vicine alla criminalità "più o meno" organizzata anche l'azione nella dimensione cyber segue – ancora – questo trend. Dalla capacità di intelligence all'offensive security, dalla difesa e la *cyber hygene* alla propaganda, ancora oggi i simpatizzanti della jihād islamica, che appar-

tengano ad Al-Qāʿida o allo Stato Islamico, fanno largo uso della dimensione cyber, motivo che comporta e giustifica un costante monitoraggio del dominio digitale da parte degli operatori a ciò preposti.

Ma l'intelligence non è solo ed esclusivamente controllo del perimetro del dominio in questione. L'intelligence costituisce un punto di forza – giustificando la sua natura – se riesce, quando può, a predire e prevenire la minaccia. Non a caso, un motto mai abbastanza considerato dell'intelligence italiana è proprio "affinché una minaccia non diventi mai una notizia". Questo è ciò che, intrinsecamente e a prescindere da quale tecnica di raccolta e analisi delle informazioni si usi, contraddistingue lo strumento intelligence dal law enforcement che – se pure in tempi più recenti si sta dotando di aspetti preventivi degni di nota – agisce solitamente ex post. L'intelligence di contro deve agire ex ante, capire i fenomeni, predire le minacce e – possibilmente – sventarle. In questo il lavoro della dottoressa Florio, premesse le indiscusse doti analitiche ma soprattutto, come detto, immaginative, è molto interessante. L'analisi delle ipotesi competitive che troverete nel lavoro difatti dimostra un elemento molto sensibile che chiunque si sia occupato di terrorismo islamico per un sufficiente numero di anni sa già. Ovvero che senza il dovuto apporto logistico – ora degli Stati, ora della criminalità "più o meno" organizzata – difficilmente anche gruppi terroristici più organizzati e storici riuscirebbero a portare avanti attacchi nel dominio digitale come, aggiungo, in quello fisico. O, nel mondo ormai *phygital*, nella congiunzione tra i due.

Questo perché il sistema di prevenzione, sia esso segreto o palese, sembrerebbe aver abbastanza tenuto, se osserva-

to in una disamina diacronica, relativa all'Italia e coprendo almeno un ventennio. Se le nuove generazioni, in tutto il mondo, sembrano meno inclini a sposare la causa della jihād segnando un punto a favore di chi ha combattuto l'odio in ogni forma possibile – anche "non convenzionale" per usare una metafora dell'allora direttore del DIS ambasciatore Massolo – il pericolo che queste saldature tornino ad essere reali rimane concreto, facendo sì che il terrorismo ritorni ad essere uno strumento geopolitico agitato da Stati non di secondaria importanza in regioni in particolar modo di interesse per l'Italia. E questo elemento, tenuto spesso riservato affinché vi possano lavorare diplomazia e intelligence lontano dai riflettori, emerge chiaro dall'analisi che vi apprestate a leggere, rimandando al tema delle guerre asimmetriche su cui non si andrà oltre.

In ambito NATO si è più o meno tutti concordi che per come sono messe le strutture operative delle principali organizzazioni terroristiche un attacco da parte loro capace di minare i servizi essenziali – che richiederebbe un elevato grado di sofisticazione – non sia al momento possibile. Di contro, non è escluso che questi soggetti possano essere aiutati nel portare avanti un compito di questo genere, anche a loro capacità offensive leggermente aumentate dovute alle grandi disponibilità che comunque la rete oggi offre, nel bene come nel male, in termini soprattutto di info e service sharing (ad esempio dark web, hackers for hire, ecc). Sorprende che le conclusioni del lavoro analitico della dottoressa Florio siano assolutamente in linea con questa visione "comune" pur essendo la sua un'analisi – per quanto metodologicamente valida e non per questo meno importante – condotta interamente sulle fonti aperte. Che rinforza le ar-

gomentazioni di chi sostiene che l'OSINT sia ormai entrata definitivamente nel novero delle principali metodologie di raccolta e analisi di informazioni al pari delle più storiche HUMINT o SIGINT, solo per citare le più note.

E se come notato i nemici rimangono quelli di sempre, in particolare USA o Israele, anche l'applicazione di un framework metodologico più "moderno" che sappia tenere conto degli aspetti digitali dà ragione alla dottoressa nel sottolineare che questo aspetto non è da sottovalutare in un'analisi all source maggiormente comprensiva di dettagli e complessità che vada quindi a stagliarsi gradualmente sui livelli strategici, in particolare quelli che riguardano la gestione dei rapporti tra Stati. E per quanto riguarda la grand strategy italiana non parliamo solo di quelli amici, come quelli menzionati precedentemente, ma anche e soprattutto quelli alleati e partner che per motivi di egemonie regionali o economico-finanziari, legati ai loro specifici interessi nazionali (che ogni Stato, dagli USA alla Russia all'Arabia Saudita fino all'Australia difende e difenderà sempre) potrebbero essere perlomeno tentati di agitare lo spettro del terrorismo, a cominciare proprio dal dominio digitale che oggi molto più di ieri assurge a componente centrale della vita di ogni Stato occidentale, compromettendo – proprio come sottolineato nel lavoro – l'erogazione di servizi essenziali che non senza difficoltà continuiamo ad erogare al cittadino e uno dei veri e principali elementi di distinzione dell'Occidente da altre aree meno fortunate del pianeta.

Infine, al termine del lavoro troverete delle buone pratiche con cui la dottoressa Vi guiderà in una serie di dovute azioni che chiudono il cerchio del suo lavoro, volte alla mitigazione di un rischio che lei – come ogni esperto – intravede

a monte dell'analisi. Sono condotte di buon senso che auspico ognuno potrà far sue da una prospettiva multidimensionale, sia che esse riguardino operazioni più di alto livello come partnership pubblico-private sia che esse riguardino aspetti più verticali come monitoraggio o mappatura delle infrastrutture critiche nazionali e relative vulnerabilità, ad esempio dei sistemi SCADA. Questo perché il terrorismo, che come vedrete nel lavoro si arricchisce di nuove categorie e sottocategorie dovute alla naturale evoluzione delle cose, come quella nel mondo digitale, si vince solo facendo sistema. A partire dalla valorizzazione di lavori come questo che non sono solo metodologicamente validi da una prospettiva accademica e operativa, ma sono infusi di una capacità immaginativa senza la quale difficilmente riusciremo a vedere oltre il gioco di specchi delle nebulose attività di chi al dialogo preferisce, ancora oggi, l'odio.

Federico Sergiani

Introduzione

L'oggetto della ricerca è il terrorismo cibernetico. Negli ultimi decenni, a livello globale, abbiamo assistito alla progressiva digitalizzazione del mondo analogico, l'alto livello di informatizzazione e interconnessione che caratterizza la società odierna ha determinato il cedimento dei tradizionali perimetri di sicurezza e ciò ha esposto gli Stati a una molteplicità di potenziali minacce da prevenire e affrontare. La dipendenza da computer, network e infrastrutture ICT (Information and Communication Technologies) ha fatto crescere il timore che il terrorismo non si limiti a usare il cyberspace solo come uno strumento per condurre propaganda, proselitismo, raccolta fondi e per organizzare attentati (comunicando anche tramite crittografia e steganografia), ma come vero e proprio veicolo di attacchi terroristici che potrebbero avere delle conseguenze rilevanti per l'integrità degli Stati. L'intento di questo studio è quello di contribuire a produrre conoscenza su un fenomeno attualmente molto dibattuto, complesso e mai ancora realizzatosi nella sua accezione "pura" nonché studiare e analizzare, partendo dal concetto generale e finendo al caso specifico, se un'organizzazione terroristica possa sfruttare mediante la sua transi-

zione dal mondo fisico a quello virtuale il dominio cibernetico come vettore per condurre un attacco con finalità terroristiche, minando le infrastrutture critiche nazionali e mettendo così in pericolo la sicurezza della nostra Repubblica. A tal fine sono state integrate metodologie, nozioni e tecniche apprese durante il corso del master SIIS (Sicurezza delle informazioni e informazione strategica) per fornire un contributo metodologico volto alla prevenzione e al contrasto della potenziale minaccia. Per soddisfare questi obiettivi la ricerca è stata suddivisa in tre capitoli, in ognuno dei quali si è seguita una logica ben precisa tentando di includere degli elementi di novità nello scenario considerato. *In primis* si è cercato di fornire una panoramica generale sullo stato dell'arte del terrorismo cibernetico sia a livello internazionale che nazionale, questa parte della ricerca è stata poi utilizzata per l'ideazione di un esempio di categorizzazione del terrorismo cibernetico al fine di circoscrivere i confini del fenomeno e stabilire un quadro statico per limitare il campo d'indagine della minaccia specifica. Inoltre, è stato riportato un Terrorist Activity Framework per individuare e mettere a confronto le attività che generalmente svolgono i gruppi terroristici sia nel mondo fisico che nel mondo digitale. Il secondo capitolo consente il passaggio dalla trattazione del terrorismo cibernetico nella sua accezione generale ad approfondire uno specifico gruppo del terrorismo di matrice jihadista, attivo nello spazio cibernetico, attraverso un caso studio incentrato sul digital jihād dell'Islamic State (IS) per il quale è stata utilizzata l'analisi OSINT integrata con la SOCMINT. In tal senso si è ritenuto necessario fornire una breve panoramica sulla terminologia inerente al mondo jihadista e alla transizione spaziale dei due gruppi più co-

nosciuti a riguardo ossia Al-Qā'ida e lo Stato Islamico (IS) studiando quando e come è avvenuto il passaggio delle due organizzazioni terroristiche nella sfera virtuale. Il secondo capitolo si conclude mediante l'incrocio del Terrorist Activity Framework e i risultati dell'analisi OSINT grazie alla quale si dimostrerà a che punto si trova l'IS nella sua potenziale metamorfosi verso il terrorismo cibernetico. Il terzo capitolo è basato sulla sicurezza nazionale, dato che generalmente un terrorista per raggiungere i propri obiettivi punta al danneggiamento o alla distruzione dei settori essenziali che costituiscono un ordinamento, ai fini dello studio è sembrato interessante analizzare quali siano le infrastrutture critiche (materiali e immateriali) italiane che potrebbero rappresentare un potenziale target per il digital jihād dell'IS provocando gravi effetti sulla sicurezza del nostro Paese sia a livello cibernetico che fisico, a tal fine ci si è serviti della tecnica di analisi strutturata ACH (Analysis of Competing Hypotheses) per concludere con un'analisi previsionale a breve e medio termine. Alla luce delle analisi svolte il terzo capitolo propone delle buone pratiche di prevenzione e contrasto in particolare al digital jihād dell'IS, per cui l'Agenzia per la cybersicurezza nazionale (ACN) potrebbe fungere da faro e simbolo di sinergia e coordinamento tra i già esistenti tre pilastri tecnico-operativi nazionali dediti alla prevenzione e repressione del crimine informatico incluso il terrorismo cibernetico.

Studi

#4 David Cavatorta, *DEDICATVM. Interazione tra compositore ed esecutore*

#5 Alberta Fabbricotti, *La protezione delle minoranze nel diritto internazionale. Attualità del tema tra corsi e ricorsi storici*

#6 Ivano Azzellino, *Gramsci, Togliatti, Berlinguer. Tre idee per il cinema e la letteratura*

#7 Davide Andrea Macario, Manuel Perdicaro, *Profili giuridici dell'odontoiatra nell'ambito della medicina estetica*

#8 Davide Costa, *Cannibalismo. Questioni di genere e serialità*

#9 Pasqualina Florio, *Terrorismo cibernetico e sicurezza nazionale. Potenziale metamorfosi della minaccia eversiva*