LUISS

Dipartimento di Scienze Politiche

Cattedra di Sociologia della Comunicazione

AVVENTO DELLA NETWORK SOCIETY:
NUOVE SFIDE CYBER E RESTYLING DELL'INTELLIGENCE

RELATORE:

Michele Sorice

CANDIDATO:

Sara Benedetti Michelangeli

Matr: 083952

Anno accademico 2018-2019

Avvento della Network Society: nuove sfide cyber e restyling dell'Intelligence

Indice:

Introduzione

Il presente elaborato ha come argomento centrale quello dell'evoluzione dei servizi di Intelligence in seguito all'entrata in gioco dei mezzi di comunicazione di massa, meglio conosciuti come ICT: interconnessioni. Inoltre, viene approfondita la tematica del terrorismo cibernetico, presa in analisi quale esempio di minaccia contemporanea prodotta da Internet.

La disamina quindi rappresenta un *continuum* analitico in cui da un lato si evidenziano i lati positivi della società dei New Media e dall'altro ne vengono messe in risalto criticità e problematiche, sia a livello sociale che a livello di sicurezza cibernetica.

Lo scopo del lavoro è quello di sviluppare in seno al lettore uno spirito critico relativo alla tematica concernente le nuove tecnologie, allertando da un lato lo schieramento composto dai cyber-entusiasti dei rischi che un'eccessiva fiducia nella rete quale strumento profetico può generare e dall'altra parte mettendo in luce la spinta propulsiva che la società di rete può creare al fine di far progredire il costrutto sociale *in toto*. È chiaro quindi come io mi ponga in una posizione intermedia tra i due estremi, motivo per cui credo nelle molteplici potenzialità e funzionalità di Internet ma in altrettante vulnerabilità dello stesso. Al fine di trovare un compromesso, il *bargaining* nel gergo delle relazioni internazionali, propongo in quest'analisi delle possibili prospettive di aggiornamento del panorama di Internet quali una maggiore cooperazione internazionale volta a rafforzare l'efficacia dei servizi di Intelligence, un maggiore controllo dei contenuti *online* al fine di mantenere un equilibrio tra lo spazio cibernetico e la realtà *offline* e un'interazione forte tra risorse elettroniche e risorse umane volte a sventare le minacce provenienti dal Web, a mio avviso complesse e composte da fattori inscindibili e inestricabili che necessitano dello studio di variabili contestuali così come dei Big Data.

La ragione che mi ha spinto a trattare un simile argomento risiede nel mio spiccato interesse per la tematica della difesa e della sicurezza a livello internazionale e nella mia forte curiosità di comprendere a fondo le radici e le motivazioni che spingono i terroristi di matrice religiosa a compiere attentati ed attacchi come quelli che a partire dall'11 settembre del 2001 sconvolgono l'Occidente. Essendo appassionata di terrorismi, ho cercato di fornire una breve spiegazione dell'evoluzione teorica ed evenemenziale che ha caratterizzato e tracciato la strada imboccata dal fenomeno terroristico, fino ad arrivare a quello contemporaneo. In particolare, ciò che ho cercato di

mettere in evidenza, è il cambiamento a livello ideologico che il terrorismo ha subito nel corso del tempo.

Come nel caso dell'ideologia in campo politico, anche nelle attività terroristiche, il *leitmotiv* non è più legato a credenze e strutturazioni ideologiche, quanto piuttosto a desiderio di dominio e interessi personali. La globalizzazione ha plasmato un nuovo modo di intendere il mondo nella sua totalità, il che ha comportato una traslazione sociologica. Io ho cercato di coglierla analizzando l'evoluzione del caso e poi fornendo l'esempio pratico dell'ISIS per rendere chiara la portata e l'ampiezza del fenomeno in questione.

D'altro canto, l'Intelligence mi interessa in quanto attività di difesa e sicurezza. L'interesse verso tale settore di studio è dipeso da un fattore territoriale. Quando ero più piccola a Civitavecchia, la mia città d'origine, aveva sede una importante Scuola di guerra dell'esercito, ora trasformata in C.E.S.I.V.A (centro simulazione e validazione), nella quale venivano formati i militari, molti dei quali poi saliti ai vertici dei vari corpi dell'esercito. Il giorno che sentii parlare di Gheddafi cominciai ad associare quella realtà cittadina a qualcosa di più grande e il mio interesse crebbe incessantemente da quel momento in poi. Il mio professore di inglese del liceo mi raccontò di come Muhammar Gheddafi fosse ancora un giovane ufficiale dell'esercito di Re Idris quando frequentò la Scuola di guerra a Civitavecchia, esercito che poi fece cadere con il colpo militare del 1969 che inaugurò la sua era. Questo fatto mi fece avvicinare al mondo delle relazioni internazionali, mi appassionai di Libia e inevitabilmente di Intelligence.

Il lavoro si compone di tre capitoli. In ognuno di essi viene introdotta una tematica, più precisamente nel primo il tema trattato è l'avvento della Network Society. Si presenta il fenomeno della globalizzazione, sia economica che tecnologica, per spiegare la realtà multiforme, dinamica e multipolare che caratterizza la società moderna. In seguito si prosegue con l'introduzione del fenomeno terroristico nel secondo capitolo e infine nel terzo ci si focalizza sull'Intelligence. Vediamo più nel dettaglio.

Nel primo capitolo viene introdotto il concetto di network society a partire dal quale si snoda il discorso relativo al cambiamento, prima di tutto sociologico, che i mezzi di comunicazione hanno determinato nella società. Infatti, con la globalizzazione dell'informazione, l'essere umano ha modificato il suo modo di relazionarsi, discostandosi sempre di più dal suo habitat sociale e nutrendosi invece della rete quale linfa relazionale e comunicazionale. Questa digitalizzazione dell'individuo ha fatto sì che la socializzazione non avvenisse più nell'Agorà bensì in Internet. Dopo aver tracciato la direzione che la massificazione della comunicazione ha imboccato, viene

introdotto il concetto di Intelligence, passando brevemente in rassegna il processo evolutivo che tale attività ha subito nel corso dei decenni e arrivando infine ai tempi recenti, in cui l'attività di prevenzione dei confini statali, storica funzione dei servizi segreti, si è tramutata in un'attività transnazionale, il cui *modus operandi* si basa sempre più sull'utilizzo delle nuove tecnologie al fine di essere efficiente nel contrasto delle minacce globali. Nell'ultimo paragrafo del primo capitolo viene analizzato il caso studio di *Wikileaks* per mostrare, nonostante i passi in avanti dei servizi di Intelligence, le criticità strutturali che essi ancora presentano. Il sito creato dall'*hacker* Julian Assange ha messo in luce le vulnerabilità dell'Intelligence in materia di protezione delle informazioni sensibili; infatti documenti privati della CIA sono stati resi pubblici senza particolari ostacoli, il che ha mostrato le carenze dell'Intelligence in ambito cibernetico e la necessità di aggiornare e ricostituire un nucleo organizzativo della stessa.

Il secondo capitolo si occupa invece di introdurre il fenomeno del cyber-terrorismo, oggi attualissimo e molto pericoloso. Il primo paragrafo mira a esplicitare il concetto di terrorismo, tracciando un percorso dell'evoluzione del fenomeno fino ad arrivare ai tempi recenti ed alla declinazione *cyber* che esso ha assunto. In seguito vengono introdotte e spiegate le modalità tramite cui i terroristi utilizzano il Web, note come stretegie *tool oriented* e *target oriented*, rispettivamente consistenti nello sfruttamento della rete quale strumento e quale arma. Successivamente viene fatta un'analisi di quanto spiegato in precedenza tramite il *caso studio* dell'organizzazione terroristica ISIS, mostrando il modo in cui gli *hackers* dell'autoproclamatosi Stato islamico si servono di Internet per portare a compimento i loro progetti, *ergo* attacchi ed attentati terroristici.

Il capitolo si conclude con un accenno ai principali attori internazionali in materia di attività di *counter-terrorism*, ovvero gli Stati Uniti, L'Unione Europea e la NATO. *In primis* vengono definite le loro linee d'azione, poi vengono messe a confronto mostrando lo scarso grado di cooperazione ed interazione dovuto a problematiche di raccordo tra di essi e infine vengono proposte delle soluzioni ipotetiche volte a rendere le attività di contrasto del terrorismo più efficaci e coese.

La parte conclusiva dell'elaborato si concentra invece sulla branca dei servizi di Intelligence nota come SOCMINT: Social Media Intelligence. Tale attività consiste nell'analisi dei contenuti dei social network quale mezzo per contrastare le attività terroristiche e non solo. Essa viene spiegata e mostrata nelle sue positività prima e vista alla luce delle sue carenze poi. In particolare, due problematiche fondamentali vengono trattate nel presente lavoro: quella nota come *signal-to-noise*

ratio, consistente nella difficoltà dell'individuazione delle informazioni realmente rilevanti all'interno della rete data l'ampia mole di dati contenuti in essa e quella della rappresentatività del campione (*sample representativeness*) . Ciò significa che i metodi statistici e computazionali di cui si serve la SOCMINT al fine di compiere un'analisi dei dati provenienti dalle piattaforme *online*, risulta a volte fuorviante dell'effettivo stato dei fatti. La statistica tralascia delle componenti analitiche fondamentali quali il contesto sociale che non possono essere eluse nell'attività di contrasto del terrorismo. A tal fine l'elaborato introduce la tematica dell'interazione della SOCMINT al metodo c.d "human-sized", cioè quell'analisi *offline* svolta dagli analisti di Intelligence.

Infine, dopo aver spiegato l'approccio "human-sized" si paragonano i metodi analitici dei servizi italiani e quelli americani , la cui principale differenza si evidenzia proprio nell'umanizzazione o nell'utilizzo solitario della SOCMINT: nel caso dell'Italia, l'interazione tra realtà *online* e *offline* appare molto sviluppata, nel caso degli Stati Uniti invece, la corrente *maistream* è quella che vede la SOCMINT in prima linea come strumento efficace in materia di lotta al terrorismo, senza bisogno di contributi analitici provenienti dal mondo oltre la rete.

Nella parte in cui espongo le conclusioni, metto in evidenza ancora una volta quanto sia difficile parlando di Internet , pervenire a soluzioni univoche e inequivocabili. Lascio quindi al lettore trarre le sue conclusioni, nella speranza di avergli fornito gli strumenti necessari per poter analizzare con spirito critico la tematica trattata e con l'auspicio di aver stuzzicato il suo interesse per l'argomento.

Capitolo primo- l'avvento della network society e il mutamento dell'intelligence

Network society: come l'arena virtuale ha riscritto le regole dell'informazione

Il mondo in cui viviamo è il mondo creato dalla globalizzazione. È impensabile immaginare di comprenderne orientamenti e direttrici se non lo si pensa in un'ottica globalizzata. Ma la globalizzazione non è solo quella economica, è anche quella dei mezzi di comunicazione di massa, ed è proprio questo l'aspetto di cui ci occuperemo in questa trattazione, perché imprescindibile per spiegare l'avvento della *network society* e per comprendere il nuovo volto dell'Intelligence moderna che la "società di rete" ha generato.

La globalizzazione dei mezzi di comunicazione di massa ha creato quello che McLuhan definisce con l'ossimoro: "villaggio globale". (McLuhan, 1964) Con questa espressione il sociologo canadese rende l'idea di un mondo , quello toccato dalla globalizzazione, nel quale il *"villaggio"*, cioè la forma primordiale di aggregazione e di abitato umano, si lega alla dimensione "globale" . In altre parole, i mezzi di comunicazione *globalizzati* rendono possibile al *villaggio* di diventare *globale* nel senso che permettono forme di interazione prima impensabili; consentono una sorta di interattività multimediale che abbatte confini e distanze e che genera quindi una dimensione in cui prevale un approccio di tipo olistico, in cui elementi prima distaccati divengono collegati. Lo spazio in cui tutto ciò avviene non è più reale, si parla piuttosto di un'arena virtuale, quella delle interconnessioni. (Gagliardi, 2019)

Da tale mutamento sociale e sociologico plasmato dalla globalizzazione dei mezzi di comunicazione di massa, è derivato il conseguente avvento della "società di rete".

Questa espressione, per dirla con Leopardi "vaga e indefinita" e sovente utilizzata dai più senza attribuzione di alcun significato preciso ed univoco, rappresenta infatti il fulcro su cui fanno leva la modernità e la società contemporanea e merita perciò di essere approfondita nella sostanza. Così come è imprescindibile cercare di addentrarsi nelle implicazioni infinite che essa comporta.

La "network society", per esprimerci nella lingua del coniatore del termine, è indefinibile unitariamente, ma il suo padre fondatore, Manuel Castells, ci ha permesso di comprenderne perlomeno il *core* fondante.

Si tratta di un spazio all'interno del quale le attività e le strutture sociali[1] principali si organizzano intorno a un sistema di reti di informazione organizzate elettronicamente. Ed è l'informazione a giocare un ruolo chiave in questa nuova realtà. Essa è l'elemento di rottura con il passato poiché è l'elemento di cui i modelli a rete si nutrono. La rete non è altro che un immagazzinatore di informazioni, le quali in essa si incontrano e generano aggregazione intorno a tematiche specifiche. La *ratio* della condivisione e della prossimità tra gli individui non è più data da una vicinanza geografica ne' territoriale ma è piuttosto il risultato di affinità semantiche, passioni e interessi in comune.[2] Le persone si raggruppano sulla base di quello che vogliono condividere: un'idea, un disagio sociale, una protesta, un dolore. (Gioia, 2018)

Costruiscono delle "immagined communities" (Anderson,1983), ovvero delle comunità fondate sulle percezioni comuni e sul bisogno di sentirsi membri di una collettività, all'interno delle quali il collante è l'identità condivisa che si genera a partire dai loro bisogni. Questo meccanismo è reso possibile proprio dalla digitalizzazione e quindi dalla possibilità di condividere informazioni nella rete; è grazie all'arena virtuale in cui circola che l'informazione assume una dimensione transnazionale, trapassando confini e barriere geografiche.

I cosiddetti New Media[3] hanno rivoluzionato il mondo. Con essi c'è stata una vera e propria variazione antropologica così come sono cambiate in egual misura le potenzialità delle persone. L'essere umano ha modificato il suo modo di essere umano, sociale, relazionale e politico. La specie ha subito una "trasformazione digitale", così come definita dall'XI rapporto del CENSIS-UCSI. [4]

Il web e i nuovi media però sono un'arma a doppio taglio. Se da un lato consentono l'abbattimento di distanze e confini e la dimensione spaziale-temporale diviene ubiqua [5], dall'altra permettono agli individui di scegliere l'informazione che vogliono recepire, evitando quella con cui non vogliono avere a che fare. Essi creano delle "filter bubbles" (Pariser, 2011) che li isolano intellettualmente

[1] La struttura sociale, nelle scienze sociali, rappresenta l'organizzazione sociale modellata nella società che è sia emergente che determinante delle azioni degli individui.

[2] Nel Web si creano delle comunità virtuali in cui gli individui condividono i loro interessi. Lo strumento attraverso cui si sviluppa tale raggruppamento è generalmente il forum, anche noto come "gruppo di discussione".

[3] Il complesso dei mezzi di comunicazione frutto delle recenti tecnologie.

[4] L'undicesimo rapporto CENSIS/UCSI sulla Comunicazione analizza le trasformazioni introdotte dall'era digitale. In particolare analizza il cambiamento delle diete mediatiche degli italiani nonché i principali mutamenti attitudinali determinati dalla *digital life.*

[5] La caratteristica principale delle reti è l'istantaneità. Nel Web il fondamento comunicativo muta radicalmente: c'è un'interazione diretta e simultanea tra gli individui.

nella propria *bolla* e li allontanano dalla necessità di interfacciarsi con qualsivoglia punto di vista conflittuale rispetto alle loro credenze e ai loro interessi. [6]

È chiaro quindi come il mondo dell'informazione sia stato radicalmente rivoluzionato dall'avvento delle nuove tecnologie. Esse hanno trasformato il modo di essere dell'informazione e il modo di fare informazione. L'implicazione più importante da cogliere rispetto alla "società della comunicazione" in cui viviamo riguarda la dipendenza che essa esercita sugli individui. Un inaspettato e improvviso *default* del flusso delle telecomunicazioni sarebbe in grado di mandare in tilt il mondo intero, con conseguenze addirittura maggiori di quelle generate da una pandemia.

Inoltre quando si parla di network society, si deve parlare necessariamente anche di *capitalismo informazionale.* (Castells, 1964) In questo spazio iperconnesso e ipercomplesso quale è il web sopravvivono i detentori del *know-how*, cioè i lavoratori ad alta specializzazione che sanno districarsi nel web e lo plasmano allo stesso tempo, mentre i *flexible workers* , ovvero i "lavoratori salariati" a bassa specializzazione rimangono intrappolati nelle grinfie di un *corpus* di informazioni che non comprendono *de visu* e che li rende vulnerabili e manipolabili. (Gioia, 2018)

La network society ha creato la *mass self comunication:* comunicazione di massa per le masse. Nella società industriale il rapporto con cui l'informazione veniva trasmessa era di *one-to-many.* Diametralmente opposto è il fondamento comunicativo della società di Internet & Co.. La comunicazione in rete è *di massa* poiché veicolata dalle reti peer-to-peer [7], *multinodale*[8] in quanto rende possibile la distribuzione e riallocazione dei contenuti *e autonoma* perché lo scambio many-to-many può essere effettuato da tutti gli *electronic devices* in circolazione, senza eccezione alcuna. Ciò significa che basta possedere un qualsiasi dispositivo elettronico per accedere alle informazioni trasmesse in rete. (Gioia, 2018)

Questa *strutturazione orizzontale* della comunicazione tipica dell'era dei *social network* inoltre è caratterizzata da un assoluto lassismo legislativo. Non esistono al suo interno regole di contenuto

[6] Si pensi alle notizie personalizzate di Facebook o alla ricerca personalizzata di Google.

[7] Le reti *peer-to peer*-, in italiano "reti paritetiche", sono reti configurate in maniera tale da poter avviare o completare una transazione (scambio) da qualsiasi nodo facente parte della rete in questione. Ciò vuol dire che tra i vari nodi c'è un rapporto di 1:1. In maniera opposta invece le reti *client-server* indicano un'architettura di rete concepita gerarchicamente, nella quale un computer *client* si connette ad un *server* per la fruizione di un servizio. Nelle reti peer-to-peer tale differenza tra *client* e *server* non esiste. Esse sono alla base del *file sharing.*

[8] La multinodalità della comunicazione di massa è da intendersi sia come *multinodalità sensoriale/ricettiva*: i segnali vengono captati da più sensi e quindi l'interpretazione dell'informazione ricevuta è il frutto dell'insieme di essi, che come *multinodalità produttiva*: i contenuti vengono trasmessi a più riceventi e con modalità differenti.

ne' di forma, non esiste un *fil rouge* dettato dalla dimensione morale ne' tantomeno figure atte a salvaguardare il rispetto di determinati limiti .

A conferma della totale mancanza di una struttura e di un ordine all'interno del mondo social sta il fatto che il leader nel mondo virtuale non è di certo colui che è formalmente riconosciuto come tale (leader politico o intellettuale) bensì colui che riesce a creare consenso intorno alla sua causa e a imporre meccanismi di solidarietà e cooperazione. Fanno scuola i movimenti di protesta quali gli *Indignados*[9] nonché le Rivolte arabe in Tunisia e Egitto, le cosiddette "Rivoluzioni 2.0" (Ghonim,2012) nelle quali i social network hanno giocato un ruolo determinante per la mobilitazione delle masse, a dimostrazione del fatto che l'interazione tra il mondo *offline* e quello *online* è di strategica importanza e che i due vivono in stretta collaborazione. Non a caso l'ondata di mobilitazione in Brasile del 2010 è stata definita come "Mobilitazione di Facebook".

Anche i gruppi terroristici fanno dei media sociali gli strumenti di veicolazione del loro *frame narrativo* nonché un mezzo per fare proselitismo.

Questa totale libertà che caratterizza l'universo delle interconnessioni comporta necessariamente l'aggiornamento dell'*agenda-setting* delle sfide e delle minacce globali nonché l'adattamento dei principali attori internazionali a questa nuova realtà 2.0.

[9] Il Movimiento M-11, ribattezzato con il nome *Indignados*, è un movimento sociale di cittadini che nel 2011 ha dato vita a una mobilitazione dal basso in segno di protesta contro il governo spagnolo allora in carica (governo Zapatero) a fronte della drammatica situazione economica in cui versava il Paese.

L'intelligence 2.0 : le nuove sfide dell'universo cyber

L'Intelligence, di cui tra poco cercherò di fornire un'adeguata definizione, rappresenta da sempre un elemento di vitale importanza per gli Stati e la loro potenza. A conferma di ciò, basti ricordare le parole di Hitler rispetto all'allora U.R.S.S: "I Russi sono esseri inferiori, ma Stalin ha un'unica dote in più di me, ovvero il suo servizio segreto."[10] (Giannuli, 2012)

Si può dedurre logicamente da queste parole che, se l'Intelligence era fondamentale prima della digitalizzazione e dell'avvento delle reti, diventa decisiva nell'iperconnesso mondo contemporaneo delle ICT. Chiaramente però, trattandosi di una società 2.0, anche l'Intelligence dovrà essere tale.

Con l'avvento della network society, la maniera di intendere l'intelligence e il suo *modus operandi* si sono radicalmente modificati rispetto all'era del "mitico" spionaggio. Occorre però, per inquadrare il mutamento, definire nella maniera più oggettiva possibile questo termine traducibile in italiano come "intelligenza", così misterioso e intrigante ,che da tempi immemori viene associato a *spy-stories* e attività amorali.

L'Intelligence è :"l'insieme delle attività finalizzate all'acquisizione d'informazioni rilevanti per la sicurezza dello Stato" (difesa.it). Il suo ruolo è quello di mantenere e salvaguardare la *salus rei publicae*[11] , sempre più a rischio nella *società aperta*[12] (Popper, 1932) quale è quella contemporanea . Ciò detto, questa attività di individuazione delle potenziali minacce alla sicurezza statale va intesa come forma di difesa preventiva, ovvero la *ratio* dei servizi di Intelligence è quella di anticipare la mossa del nemico, in termini strategici, tenerlo sotto scacco. In una realtà multiforme e dinamica come è quella della rete, però, le minacce nonché la loro individuazione, risultano essere molto più variegate e complesse rispetto allo storico pericolo per la sicurezza nazionale quale era l'attacco militare nell'era precedente al *cyber-space*. (Giannuli, 2018)

Prima delle interconnessioni, l'Intelligence era quella militare e l'azione era quella dello spionaggio e dei messaggi criptati, tecnica utilizzata sin dal Medioevo dagli "007 lagunari", ovvero gli agenti segreti della Serenissima Repubblica di Venezia. (Giannuli, 2018) Oggi invece le sfide più pericolose sono senza dubbio quelle cibernetiche. Le minacce cyber sono potenzialmente devastanti , tanto che il "rischio cyber" è stato inserito da qualche anno nella lista dei "TOP Risks" stilata dal

[10] Hitler pronunciò queste parole in riferimento all'informazione confidenziale pervenuta all'esercito russo da una spia riguardante i giapponesi che avrebbero attaccato solo gli americani.

[11] Si intende la salvaguardia della sicurezza di un determinato territorio.

[12] Con l'espressione *società aperta* qui si vuole intendere una società caratterizzata da pluralismo e dinamismo, una società globalizzata.

World Economic Forum. (Guida, 2019) Ecco quindi che entra in gioco la *cyber-intelligence* per far fronte ai pericoli dello spazio virtuale. Lungi dall'essere unitariamente definibile, la *cyber-intelligence* può essere inquadrata come un connubio tra l'Intelligenza classica e l'informatica . La dimensione *cyber* dell'Intelligence permette di condurre l'azione di raccolta di informazione a scopo preventivo, sua storica funzione, tramite lo spazio cibernetico. (Brando, 2018)

Questo è necessario dal momento che nella società odierna la rete rende gli *unexpected events* non più inaspettati e che criminali, terroristi, ladri e guerriglieri usano il web quale strumento per compiere le loro azioni malevole, generando minacce di dimensione globale note rispettivamente come *cyber-crime, cyber-terrorism e cyber-warfare*; minacce tra l'altro che scavalcano agilmente i confini statali, e che mettono a rischio imprese, persone e intere comunità. Infatti, gli attacchi perpetrati dai criminali di oggi non sono più solo attacchi militari. Sono spesso anche attacchi informatici, volti a colpire la infrastrutture critiche di un Paese generando crisi e conseguenti ripercussioni in tutti gli ambiti socialmente rilevanti per esso.

Queste nuove sfide *cyber* transnazionali e globali devono quindi essere classificate e successivamente contrastate. L'Intelligence informatica è chiamata a farlo.

L'analisi della *cyber-intelligence* diventa quindi *in primis* l'analisi delle *threats* informatiche e il suo scopo quello di individuarle e sventarle. Secondo la definizione della NATO, la *cyber-threat intelligence* è : "Il prodotto risultante dalla raccolta e dell'analisi delle informazioni sull'ambiente, le capacità e le intenzioni degli attori, finalizzato all'identificazione delle minacce e a supportare il processo decisionale". (Caforio, 2018)

Resta però un problema, quello delle vulnerabilità della *cyber-intelligence*. L'adattamento dei servizi alla dimensione virtuale del web , sebbene fondamentale, ha ancora delle falle. D'altra parte, se avesse un'efficacia completa non si porrebbe il problema ne' delle minacce cibernetiche , ne' tantomeno della *cyber-security*.

Debolezze dell'Intelligence nell'era delle interconnessioni: Wikileaks come emblema

Nel mondo moderno, cioè quello virtuale, le incognite cui l'Intelligence deve far fronte sono molteplici e il più delle volte indecifrabili. Tra le sfide maggiori per i nuovi analisti dei servizi si pone quella della segretezza. Se da un lato abbiamo assistito a uno *switch* della nuova Intelligence verso l'utilizzo di un *corpus* di fonti non più solamente segrete ma anche aperte (tecnica nota *come open source intelligence*), dall'altro documenti top-secret, coperti dal segreto di Stato, sono diventati fonti per così dire "*open-source"*[13], ma non per mano dell'Intelligence, bensì a suo discapito. Emblematico in tal senso è il caso *Wikileaks.* Questa vicenda ha evidenziato l'incapacità dei servizi contemporanei di stare al passo con le molteplici sfide *cyber* cui devono far fronte, *ergo* dovrebbero. Ma procediamo per gradi.

Wikileaks nacque nel 2006 per mano di Julian Assange, un matematico e *hacker* australiano, che diede vita a questo sito senza scopo di lucro volto a garantire la trasparenza globale, a de-secretare il segreto. In tale piattaforma *online* non venivano pubblicate notizie ma veri e propri documenti segreti e quindi , sulla carta, inaccessibili e irreperibili, tra cui documenti della CIA.

Wikileaks ha reso di pubblico dominio, tramite Twitter, praticamente tutta la capacità di hackeraggio del *Center for Cyber Intelligence* statunitense. È stata pubblicata in rete una collezione di 8.761 pagine di documenti della CIA, nota con il nome di *Vault 7* e che rappresenta la *leak* (fuga di notizie) più grande di sempre. Evidentemente il sistema di segretezza statale americano non ha funzionato a dovere, anzi è stato esposto al collasso. (Killelea, 2017)

Il punto cruciale che questo lavoro vuole evidenziare, lasciando fuori dal dibattito qualsiasi giudizio di valore relativo al merito della vicenda, è quello della estrema debolezza che l'Intelligence digitale americana ha dimostrato in questo caso, totalmente incapace di proteggere le informazioni di suo dominio, che sono state rese reperibili per e da tutto il mondo con una facilità estrema. E parliamo dei servizi più evoluti al mondo in termini di disponibilità economica nonché di mezzi digitali a disposizione. Il nodo della questione è inestricabile. Se degli *hackers* senza alcuna preparazione in ambito militare ne' addestrati ad essere analisti d'Intelligence, sono riusciti a tenere sotto scacco l'apparato informatico degli Stati Uniti d'America e a mettere in pericolo la sicurezza statale, il futuro della *cyber-Intelligence* è chiaramente da riscrivere. Infatti, il punto su cui riflettere sta nel fatto che quella fuga di notizie ha provocato la proliferazione di *malaware* e virus, che sono diventati di dominio pubblico e utilizzabili da chiunque, dalle cyber-mafie ai cyber-terroristi.

[13]La open source intelligence (OSINT) è l'attività di raccolta di informazioni tramite la consultazione di fonti pubbliche.

(Killikea, 2017) Quella pubblicazione ha reso le *cyber-armi* della CIA reperibili da chiunque e in qualsiasi parte del mondo, esponendo quindi la sicurezza statale a minacce provenienti da ogni dove. La *digital-age*[14] rischia di provocare un crollo dei servizi di tutto il mondo, o perlomeno un indebolimento di essi rispetto alle minacce globali che li tengono sotto scacco, tra cui in primo piano c'è quella del *cyber-terrorism*.

[14]Per *digital age* si intende la società di Internet, quella basata sulla comunicazione tramite l'utilizzo delle ICT.

Capitolo secondo - Le minacce del mondo cibernetico: cyber-terrorism

Cyber-terrorism: il nuovo terrorismo hi-tec

Il Web non ha solamente riscritto le regole dell'informazione; esso ha anche trasformato l'assetto geopolitico mondiale. La geopolitica è lo studio dei fattori geografici che influenzano e condizionano l'azione politica ed oggi è diventata sempre più geoinformazione[15] piuttosto che geocontrollo[16] (Colonna Vilasi, 2011). Se essa non è più legata tanto ai confini e al potere militare quanto alla globalizzazione dell'informazione, è chiaro che anche le minacce all'ordine mondiale contemporaneo saranno legate a questa nuova dimensione 2.0 della geopolitica. Il *cyber-terrorism* ne è la prova. La dimensione *globalizzata* del terrorismo è il prodotto di un mondo che dalla caduta del muro di Berlino in poi si è tramutato in uno scenario globale multipolare in cui i giocatori non sono più solo l'allora U.R.S.S e gli Stati Uniti, ma dove piuttosto si inserisce una molteplicità di attori transazionali di natura differente che soppianta la prevedibilità del precedente equilibrio bipolare e dove la parola chiave è incertezza. (Colonna Vilasi, 2011) La dimensione statale diviene sempre più marginale e in via di decostruzione, lasciando spazio ai detentori del *know-how* e dei mezzi di comunicazione di massa. Il cambiamento rivoluzionario introdotto dalla globalizzazione infatti, nonché quello che ha stravolto la concezione e la maniera di intendere il mondo contemporaneo, è proprio lo slittamento del potere dall'uomo politico agli architetti della *network society*. Sono loro ad avere in mano il *know-how* e soprattutto il *soft power*[17] (Nye, 2004), che in un mondo così dinamico e *in fieri* risulta essere determinante e più rilevante del tradizionale *hard power* militare. La dimensione *soft* del potere consiste nella capacità di persuasione e di mobilitazione delle persone. Chi lo detiene è colui che è in grado di plasmare le coscienze e orientare le personalità. Per esemplificare tale concetto basti pensare a Mark Zuckerberg e al suo potere in materia di sensibilizzazione, polarizzazione e influenza. Se lo si paragona a Hillary Clinton non vi è ombra di dubbio che l'ex First Lady ceda il passo al gigante di Facebook per l'impatto che egli ha sulla gente.

Se da un lato troviamo i *patron* dei social network a muovere i fili del mondo globalizzato, dall'altra però ci sono anche tutti coloro che anche non essendo *patron* padroneggiano il Web come

[15] Per il concetto di geo-informazione si rimanda al seguente articolo: https://www.swisstopo.admin.ch/it/conoscenze-fatti/geoinformazione.html

[16] Con il termine geo-controllo si vuole rimandare all'interpretazione della geopolitica in senso classico quale disciplina che studia le relazioni tra la geografia fisica, la geografia umana e l'azione politica

[17] Si veda: https://www.belfercenter.org/sites/default/files/legacy/files/joe_nye_wielding_soft_power.pdf

se ne fossero gli *owners* e che nella concretezza ne divengono i leader carismatici, quasi delle guide spirituali. Il mondo post-bipolare infatti ha dato vita, oltre che alla decostruzione del sistema Stato, ad un fenomeno praticato dagli attori transnazionali noto come terrorismo di matrice confessionale. Questa declinazione dell'azione terroristica trae la sua forza, la sua legittimità e il suo consenso dallo spazio virtuale. Infatti gli esponenti del terrorismo religioso odierno sono sempre più cyber-terroristi, maestri nello sfruttare le potenzialità e allo stesso le vulnerabilità della rete.

Il cyber-terrorismo può essere considerato come l'evoluzione del terrorismo tradizionale, o meglio il suo slittamento nello spazio cibernetico. Per comprenderne le sfaccettature e le diramazioni bisogna fare un *incipit*. Il terrorismo è un fenomeno datato, tanto che il primo *suicide-bombing* della storia fu Sansone all'epoca dei Filistei[18] (Campagnoli, 2017). Con l'avvento della modernità, però, il terrorismo ha modificato il suo *modus essendi*, fino ad assumere la sua connotazione di terrorismo transnazionale moderno[19]; é sulla base del terrorismo per così dire *globalizzato* che si è arrivati a parlare di *cyber-terrorism* (Colonna Vilasi, 2011). Tale termine è stato coniato da Berry Collins per descrivere gli atti terroristici che hanno luogo nel *cyber-space*. Non esiste una definizione più specifica dal momento che come evidenziato precedentemente, lo spazio virtuale e di conseguenza tutti i fenomeni che ne discendono, sono privi di regole e dettami giuridici. Non esistendo un quadro normativo, l'interpretazione del fenomeno è variabile.

Il punto fermo però è che il *cyber-terrorism* è oramai una tecnica utilizzata da tutte le organizzazioni terroristiche in circolazione, perché la rete diviene vitale per la loro sopravvivenza e per il successo delle loro battaglie. La *cyber-war* introduce una novità importante: si gioca su diversi campi d'azione, non su terreni materiali. Il ruolo della dimensione virtuale è importante poiché *in primis* determina una traslazione continua e spesso inscindibile tra reale e virtuale un po' come nel nastro di Mobius[20] (Campagnoli, 2017) , in *secundis* permette la formazione di grovigli di reti che generano il *modus comunicandi* tra le varie cellule terroristiche: grazie a questa connessione transnazionale i terroristi coordinano le loro azioni e anche i c.d *one actor* o l*one wolf*[21]

[18] Sansone fu un personaggio biblico. Le sacre scritture narrano che egli si suicidò per far crollare il tempio di Dagon, luogo di culto dei Filistei, dopo essere caduto loro prigioniero.

[19] Con questa espressione si intende sottolineare la dimensione internazionale del terrorismo preso in esame in questo lavoro.

[20] Il nastro in questione deve il suo nome al matematico tedesco August Ferdinand Mobius, il quale scrisse un trattato sui poliedri in cui introdusse una figura geometrica particolare rappresentata da una superficie allungata ritorta di centoottanta gradi con una sola faccia e un solo bordo. Tale figura, proprio a causa delle sue caratteristiche strutturali, è utilizzata per alludere al passaggio continuo che avviene tra reale e virtuale nel cyberspazio.

[21] Con queste espressioni si vuole far riferimento a quegli attacchi terroristici condotti da singoli individui e non da un'organizzazione terroristica.

hanno la possibilità di seguire le indicazioni dei loro leader emozionali, nel senso che rappresentano per loro dei mentori, per approntarsi ad attentare. Questo è il motivo per cui ultimamente tutti gli attacchi terroristici di matrice islamica vengono rivendicati seppur condotti da cellule solitarie e distaccate dall'organizzazione che si propugna come mandante. I terroristi spacciano tali azioni come comunque ispirate dalla propaganda e dai messaggi lanciati sul Web o almeno vogliono farlo credere al nemico, in maniera tale da generare in lui un senso di perdizione e di paura sempre maggiore. La *ratio* della rivendicazione degli attentati svolti dai c.d cani sciolti è quella di far passare un messaggio chiaro: il pericolo è sempre dietro l'angolo, i "fedeli" agiscono anche da soli, non sei al sicuro mai.

Inoltre la rete alimenta il terrorismo stesso *poiché il terrorismo rappresenta un modo di comunicare (seppur violento) e per esistere necessita della comunicazione.* (McLuhan, 1964) Il *cyber space* è il teatro in cui il terrorista attua la sua strategia comunicativa violenta. Egli emette un messaggio (emittente) e il pubblico lo riceve (ricevente). Il messaggio generato assume la sua connotazione violenta dal momento che c'è un ricettore su larga scala: il pubblico del Web e grazie al contenuto del messaggio stesso che funge da *generatore di potenza* di esso: natura dell'attacco terroristico, localizzazione, atrocità, identità delle vittime. [22] (Campagnoli, 2017)

Infine la rete amplifica la risonanza delle parole dei terroristi, permette la loro diffusione da un capo all'altro del mondo solamente con un *click* e quindi in tal senso il web globalizza il terrorismo e soprattutto *globalizza la violenza terroristica*.[23] (Buoncompagni, 2016). È importante sottolineare questo aspetto, perché i *cyber-terrorists* mirano a sconvolgere il nemico tramite la diffusione nel web dell'utilizzo della forza. Usano la condivisione della violenza come *weapon of psychlogical warfare*[24] (Campagnoli,2017). I messaggi circolanti nell'ubiquità della rete incrementano la pericolosità del terrorismo nonché la sua capacità di attecchimento in termini di seguaci e simpatizzanti, tanto da arrivare a parlare di un vero e proprio *spettacolo del terrorismo e terrorismo dello spettacolo* (Braudillard,1976). L'azione terroristica viene spettacolarizzata, viene messa sotto i riflettori di tutto il mondo e quindi mediatizzata. Esempi chiari ed evidenti ne sono gli innumerevoli video postati *online* dagli adepti dell'ISIS in cui si ritraggono decapitazioni e violenze

[22]Si ricordino le osservazioni di DE GRAFF e SCHMID: " La violenza, per diventare terroristica, richiede dei testimoni." (A.P. SCHMID, J. DE GRAFF, *Violence as Communication: Insurgent Terrorism and the Western News Media* (Beverly Hills, CA.: Sage Publications, 1982)

[23] Per approfondire il concetto si rimanda a : https://www.academia.edu/29232657/Violenza_contemporanea_e_cyberterrorismo-Buoncompagni.pdf

[24] Sul punto si consulti*:" I nuovi volti del terrore: dal terrorismo islamico al cyber terrorismo, fenomenologia di una perturbante forma di violenza "* M.N CAMPAGNOLI, pag.24.

di ogni genere. Questo *modus operandi* rende il nemico vulnerabile e insicuro e più facilmente attaccabile. La sicurezza quindi diventa sempre più una questione psicologica ed il terreno per i terroristi sempre più fertile.

La conflittualità *cyber* inoltre introduce un elemento innovativo importantissimo: la guerra *asimmetrica.* A partire dall'11 Settembre 2001, quello che ha contraddistinto gli attentati terroristici è stata proprio l'imprevedibilità degli attacchi. Se non c'è modo di individuare un nemico non si può reagire, si può solo rimanere inermi ed attoniti. *L'asimmetria informazionale* riguardo al nemico da combattere genera un gioco a somma zero in cui gli attori non si confrontano in condizioni di parità ne' in ossequio delle medesime regole. Il terrorista diviene imprevedibile e incontrastabile in quanto non lo si conosce e quindi detiene un vantaggio strategico. (Campagnoli, 2017)

Come disse Sun Tsu :" se non conosci il nemico e nemmeno te stesso, soccomberai in ogni battaglia."

Nel caso delle Torri Gemelle, l'Occidente e in particolare gli Stati Uniti facevano leva sul potentissimo arsenale militare di cui disponevano per difendere i propri confini materiali, ma non avevano considerato il fattore della guerra *online* tramite cui quell'attacco venne preparato e coordinato, non ne erano a conoscenza (asimmetria informazionale) e quindi si trattò di un episodio di *asimetric warfare* in cui l'America soccombette.

Il terrorismo *cyber* può essere definito anche come terrorismo *Hi-tec* poiché il fattore tecnologico è imprescindibile in fasi e livelli differenti. Non solo il mondo cibernetico permette ai terroristi 2.0 di fare proselitismo e attività di *fund-raising* ma consente loro anche di utilizzare la tecnica del *social engineering*, cioè di creare identità inesistenti, travestirsi, camuffarsi e quindi sfuggire ad ogni controllo delle autorità.

Nel paragrafo successivo infatti verranno analizzate le due tecniche principali di utilizzo del Web da parte dei cyber terroristi.

Come i terroristi usano il web: rete come arma: ”target oriented” e come strumento: ”tool oriented”

Assodato che i terroristi moderni trovano la loro linfa vitale nel Web, è importante capire come lo utilizzano. In particolare, vediamo come le organizzazioni sovversive sfruttano la rete come arma e come obiettivo da un lato : strategia del “target oriented” e come invece utilizzano il *cyber-space* quale strumento sull’altro versante: modalità nota come “tool oriented”. (Rapporto UNODC, 2012).

Il quadro è molto più complicato di quanto potrebbe apparire a primo impatto, nonché ricco di implicazioni e sfumature.

In generale, possiamo dividere le attività terroristiche nel web in 6 macrocategorie che inquadreremo nell’ottica delle strategie *target oriented o tool oriented* prima e che analizzeremo singolarmente al fine di comprenderne le diverse e molteplici diramazioni poi.

La strategia *tool oriented* identifica 4 principali macro aree di azione da parte dei cyber terroristi che sono definibili come le attività di: *propaganda*, *fund-raising*, *addestramento (training)* e *pianificazione*. Le altre 2 macro aree rientrano invece a far parte di quella categoria di interventi definibili nel quadro dell’utilizzazione della rete come arma, ovvero nella *target-oriented strategy*, e sono note come *esecuzione* e *cyber attacks*. (Rapporto UNODC, 2012)

Iniziamo con l’analisi del Web come *tool.* In particolare con l’attività della **propaganda**, la più complicata da definire e la più ricca di implicazioni. In primo luogo occorre identificare le diverse direttrici della propaganda terroristica *online.* Infatti esiste la propaganda volta al *recruitment* di nuovi adepti, quella di *radicalizzazione,* quella di *incitazione al terrorismo* e quella di *narrazione*. I punti comuni a tutte le forme di propaganda *cyber* sono una retorica estremista e un *frame* narrativo violento. Ciò vuol dire che a prescindere da quale sia lo scopo, il *vulnus* della propaganda seguirà sempre una stessa logica atta a ingenerare ansietà nel nemico tramite la condivisione di atrocità. Ma entriamo più nel dettaglio. Quando il *target* della propaganda si identifica nelle reclute potenziali, il messaggio da trasmettere consiste in un’esaltazione dei tratti distintivi dell’organizzazione e quindi dei suoi punti di forza. L’immagine da veicolare è quella del terrorista come salvatore, come persona giusta chiamata ad infliggere la meritata pena al nemico infedele e per farlo vengono esaltate le caratteristiche di un combattente integro, dedito alla causa e fiero ed orgoglioso del suo credo. In genere tali messaggi volti a rintracciare nuove reclute vengono indirizzati ad un *audience* formato dai giovani e dai gruppi sociali marginalizzati, che risultano essere le categorie più

facilmente manipolabili e convincibili da un punto di vista psicologico. Il sistema valoriale di questi individui appare meno radicato agli occhi dei terroristi e quindi agilmente destrutturabile.

La propaganda di *radicalizzazione* è piuttosto simile a quella del *reclutamento*, con la sola differenza che mira ad essere più incisiva e quindi più cruenta da un lato e più ideologica dall'altro. Essa ha lo scopo di plasmare gli individui, per cui il messaggio che deve trasparire è quello di una causa e un fine nobili e di un combattente eretto a divinità.

Per quanto riguarda invece la propaganda volta *all'incitamento al terrorismo*, si potrebbe definirla come una vera e propria *call for action*[25] e in questo caso la strategia è quella di sottolineare i motivi che spingono alla battaglia. Il gioco è quello di mettere in cattiva luce il nemico.

L'altra faccia della medaglia è invece rappresentata dalla propaganda rivolta non agli adepti e ai simpatizzanti bensì agli oppositori. Essa ha quindi natura intimidatoria; stessa *ratio* riscontrabile anche nel caso della propaganda rivolta alle vittime e alla comunità internazionale.

La diffusione dei contenuti propagandistici avviene tramite la creazione di siti web creati *ad-hoc*, tramite giornali *online* e *forum*, mediante i Social Network e i canali per la trasmissione di contenuti audio e video quali YouTube e RapidShare.

Sempre nell'ottica dell'utilizzo dello spazio cibernetico quale *strumento* troviamo l'attività di **fund-raising**. L'azione di raccolta fondi dei terroristi del Web avviene principalmente tramite 4 modalità: *l'e-commerce*, la sollecitazione diretta, le organizzazioni caritatevoli e lo sfruttamento dei pagamenti *online*. Il commercio *online* consta della vendita di libri, contenuti audio ed altri oggetti ai *supporters* con il duplice scopo di ricevere denaro e rincarare la dose del *brain-washing*[26]. Per quanto riguarda la *sollecitazione diretta* si parla di esplicite richieste di donazioni tramite l'invio di e-mail di massa piuttosto che tramite chat specifiche. Il caso dei *pagamenti online* invece si sostanzia nel furto d'identità e carte di credito o altre attività fraudolente. Infine la tecnica dello *sfruttamento delle organizzazioni caritatevoli* consiste nella creazione di organizzazioni formalmente legittime e con scopi all'apparenza benefici quali obiettivi umanitari piuttosto che filantropia, che in realtà vengono utilizzate per finanziare il terrorismo. Esempi ne sono la *Global*

[25] L'espressione *call for action* è tipica del gergo del web marketing. Frasi quali: "scarica ora", "acquista ora" e "leggi di più" sono esempi di *call for action*. Nel presente lavoro con la suddetta espressione si vuole indicare quell'attività di incitamento al terrorismo consistente nella trasmissione di messaggi inneggianti a compiere azioni terroristiche.

[26] Il *brain washing*, in italiano lavaggio del cervello, è una teoria secondo quale un soggetto può essere indottrinato al punto tale da distruggere le sue credenze e le sue affiliazioni e in modo che diventi incapace di pensare autonomamente.

Relief Foundation e la *Benevolence International Foundation*, entrambe utilizzate per finanziare azioni terroristiche in Medio Oriente.

Terza attività *tool oriented* è quella dell'**addestramento**. Ultimamente il *training* delle reclute è diventato sempre più virtualizzato, nel senso che Internet rappresenta sempre più uno strumento di diffusione di informazioni pratiche riguardanti le modalità di adesione a una determinata organizzazione terroristica o la costruzione di un ordigno esplosivo. Le piattaforme *online* vengono sfruttate, *inter alia*, per diffondere tecniche e metodi per commettere un attacco terroristico. Il magazine online *Inspire*[27] pubblicato dall'organizzazione Al-Queda nella penisola Arabica ne è un esempio. In esso vengono pubblicati contenuti ideologici diffusi dai leader dell'organizzazione e articoli riguardanti le azioni pratiche da intraprendere per portare a compimento un attentato terroristico (Marro, 2016).

Infine c'è l'attività della **pianificazione**. In questo caso lo sfruttamento del *cyber-space* è *tool oriented* nel senso che la rete viene utilizzata per pianificare attacchi e coordinarli, per instaurare contatti tra organizzazioni diverse ed identificare il *target* di un attentato. Il *planning* è fatto tramite *preparatory secret communication*, cioè l'utilizzo di strategie comunicative anonime basate sulla creazione di account di posta elettronica. In pratica i terroristi creano dei *draft messages* che non vengono inviati ma che rimangono, per dirla in gergo informatico "dead dropping"[28], cioè vengono sviluppati ma poi rimangono formalmente inutilizzati, come una bozza. In realtà tali messaggi sono accessibili da qualsiasi postazione Internet del mondo se si è in possesso della password per accedervi, ma allo stesso tempo non venendo inviati non lasciano alcuna traccia della loro esistenza.

In aggiunta a tale meccanismo, i *cyber-terrorists* utilizzano anche strategie comunicative ancor più sofisticate. Essi lavorano con la crittografia e utilizzano *software* anonimi in maniera tale da aggirare l'IP (Internet Protocol[29]) e da reindirizzare la comunicazione verso giurisdizioni che godono di una bassa protezione in materia di controllo delle attività terroristiche. Infine gli *hackers*

[27] Sul punto si consulti: https://www.ilsole24ore.com/art/mondo/2016-07-19/inspire-magazine-terrorismo-islamico-che-ispira-lupi-solitari-164036.shtml?uuid=ADrZr4u&refresh_ce=1

[28] Con l'espressione *drop-dead* si intende, con riferimento agli apparecchi elettronici, la capacità di trasmettere informazioni in maniera segreta tramite la creazione di messaggi apparentemente inesistenti(dead) , ma realmente ed effettivamente circolanti. È come se tali messaggi rimanessero sempre archiviati, tuttavia risultano sempre accessibili e consultabili dagli autorizzati.

[29] L'Internet Protocol(IP) è uno dei protocolli di Internet. Esso è fondamentale perché i messaggi in rete vengano inviati correttamente dal mittente al destinatario. Si può paragonare, al di fuori del cyberspace, alla figura del corriere, ovvero colui che consegna i pacchi spediti e si accerta che arrivino al *destinataire*. Per approfondire si veda: https://www.ionos.it/digitalguide/server/know-how/che-cose-il-protocollo-internet-definizione-di-ip-co/

si servono anche della tecnica della stenografia, attraverso cui nascondono i contenuti multimediali quali immagini, *files* audio e video. Questa è per c.d la parte segreta del *planning*, quella oscurata. Ad essa però si affianca anche la *publicly avalaible information.* Questa tecnica consiste nella riutilizzazione per fini illeciti da parte dei terroristi di informazioni sensibili pubblicate in Internet. (Rapporto UNODC, 2012) La reperibilità di tali dati è possibile grazie a dei motori di ricerca che recuperano e collezionano le informazioni provenienti da migliaia di *WebSites*. Anche applicazioni quali *Google Earth* vengono utilizzate dai terroristi per ricavare informazioni logistiche ed organizzare i propri attacchi. È stato il caso degli attacchi di Mumbai del 2008, in cui le mappe digitali di tale applicazione sono state utilizzate per identificare la localizzazione precisa degli obiettivi nel mirino degli attentatori.[30]

Se fino ad ora si è cercato di fare chiarezza su di Internet quale mezzo *tool oriented* , passiamo ora ad occuparci della sua funzione quale arma. La strategia *target oriented* rappresenta infatti l'insieme di quelle attività il cui scopo è di creare un danno, un disagio alle infrastrutture informatiche di un sistema. In particolare riscontriamo due attività principali con tale fine: l'*esecuzione* e i *cyber-attacks*.

L'**execution** consiste nella co-partecipazione di Internet e nella coordinazione da parte della rete dello svolgimento dell'attacco fisico. Le Torri Gemelle ne sono un chiaro esempio. In quell'11 settembre del 2001 fu proprio la rete di *cyber terrorists* a garantire la riuscita dell'attacco tramite il coordinamento che gli *hackers* di Al-Queda fornirono prontamente agli attentatori fisici.

Ultimo ma non ultimo elemento del cyber terrorismo è quello degli **attacchi cibernetici**. Il *cyber-attack* è il deliberato sfruttamento dei *networks* per distruggere un sistema informatico o un'infrastruttura al fine di lanciare un attacco. Esempio di *cyber-attack* fu quello che si verificò nel 2012 in Israele. Numerosi siti Web simbolici per il Paese tra cui, ad esempio, il sito della borsa israeliana: la Tel Aviv Stock Exchange , nonché il sito della compagnia aerea di bandiera: la EL AL , vennero danneggiati e infettati. Gli *hackers* ottennero così l'accesso a migliaia di carte di credito e credenziali di cittadini israeliani. (Rapporto UNODC, 2012)

Ora che il *cyber terrorism* è stato inquadrato e descritto *ex aequo* nelle sue due componenti strutturali e quindi nella genericità del fenomeno, passiamo ad analizzare il caso specifico di un'organizzazione terroristica contemporanea che della dimensione *cyber* ha fatto il suo *focus*, l'ISIS.

[30] https://www.ilsole24ore.com/art/SoleOnLine4/Tecnologia%20e%20Business/2008/12/google-earth-attacchi-mumbai.shtml

Case study: ISIS, il "jihadismo globalizzato"

Il "jihadismo globalizzato" (Weiman, 2012) è da intendersi come quella forma di fondamentalismo islamico comparsa sulla scena mondiale dagli anni 2000 in poi, che fa delle reti socio-virtuali la sua principale risorsa e che identifica il *far enemy*, inteso come il nemico d'Occidente, quale bersaglio da colpire *prima facie*.

In altri termini la *globalizzazione del jihadismo* è da considerarsi come la declinazione concettuale che il terrorismo ha abbracciato in seguito all'avvento della *network society*. Con essa è stata introdotta una nuova dimensione intellettuale: la cultura digitale, che ha radicalmente modificato il modo di intendere il terrorismo e di fare terrorismo. Con la *digital culture,* infatti, è nato il *cyber-terrorism* e si è arrivati a parlare di *globalizzazione dell'attacco*. (Buoncompagni, 2016)

L'ISIS è un chiaro esempio di *jihadismo globalizzato,* in quanto incarna totalmente sia la dimensione *cyber* che l'attacco globalizzato, ma prima di occuparci del sedicente Stato Islamico e della *cyber-war* da esso instaurata, è necessario fare chiarezza sul concetto di fondamentalismo e sugli avanzamenti teorici che il terrorismo di matrice religiosa di cui si sta parlando ha subito nel corso del tempo.

Le origini del militantismo islamico inteso quale adozione alla causa jihadista sono da ricercarsi *in primis* negli sviluppi ideologici e evenemenziali che hanno contraddistinto l'Islam e la sua interpretazione: il fondamentalismo islamico come questa disamina intende considerarlo, ovvero quale affermazione politica dell'Islam e quale autorità in cerca di un'opposizione credibile alla misreligiosità [31] degli infedeli, prende piede negli anni '70 come provento di due variabili causali: da un lato va inteso come risposta a quel *vaccum* lasciato dalle fallimentari ideologie laiche ed allogene[32] che i regimi mediorientali post-coloniali si accingevano a far proprie. Quelle ideologie infatti subirono evidenti e pesanti débâcles sul piano internazionale, tanto in ambito sociale ed economico in termini di disuguaglianze sociali e allocazione delle risorse quanto sul versante simbolico. Dall'altro lato va inquadrato come un confronto/scontro con l'Occidente che aveva generato un grande fermento nel mondo arabo-islamico, tanto che inizialmente il *leitmotiv* era rappresentato da una rivitalizzazione e un rilancio della cultura islamica rispetto a quella

[31] Con il termine misreligiosità si vuole intendere in questo contesto non colui che è scettico in materia di religione o una persona contraria all'accettazione di una fede, quanto colui che non abbraccia i precetti dell'dar-ahl-Islam.

[32] Si faccia riferimento al regime egiziano di Nasser, c.d nasserismo, fondato sul panarabismo e sul socialismo. Tale ideologia laica si rivelò fallimentare tanto localmente parlando quanto sulla scena internazionale(guerra dei sei giorni). A partire da questa disfatta cominciò ad essere pensato il "ritorno all'Islam" inteso come rifiuto della laicità e delle culture allogene.

occidentale tramite un processo avanguardista e lungimirante. Ben presto però, questa spinta riformatrice volta alla formazione di un panislamismo moderno [33] venne soppiantata e l'elemento teoretico abbandonato. La declinazione che il fondamentalismo abbracciò divenne quella apologetica, ovvero legata all'esaltazione di un pensiero e alla sua imposizione più che a un percorso modernizzatore e rivoluzionario alimentato da un'ideologia forte. La retorica autoreferenziale e celebrativa su cui i fondamentalisti islamici imperniarono la loro orazione fu *tout court* quella secondo cui : "il sistema si abbatte, non si cambia" e in cui l'egemonia è sovraordinata all'ideologia. Ma procediamo con ordine al fine di tracciare l'evoluzione da Islam ideologico a Islam come progetto politico-istituzionale e imposizione di un modello (quello del *modus vivendi* islamico). (Carenzi, 2017)

Nel contesto sopra descritto, tra insofferenza verso gli occidentali e rifiuto della laicità, si cominciò a far strada il motto del "ritorno all'Islam" nel senso della necessità di un ritorno a uno Stato realmente islamico. La maniera cui i predicatori dell'Islam integro facevano appello per ricrearlo si sostanziava nel *jihad* armato, ovvero un combattimento contro i miscredenti. L'aurea età califfale caratterizzata dalla *tawhid*[34]: unicità divina, rappresentava il modello cui dover ritornare, scacciando così i demoni della *shirk*[35]: il politeismo e restaurare la decadente casa dell'Islam: dar-al-Islam. (Carenzi, 2017)

Inizialmente però, ai tempi della predicazione di Maometto, il *jihad* era tutt'altro che uno strumento di lotta armata, infatti significava "sforzo" ed indicava lo zelo e l'impegno che il fedele doveva impiegare per combattere il paganesimo[36]. In questa fase la violenza era perciò ancora latente. L'accostamento del termine *jihad* a quello di combattimento fece la sua entrata in scena, seppur ancora inteso come difensivo e reazionario, con la morte del Profeta e infine assunse la sua connotazione di guerra di conquista ed espansione con la creazione del Califfato. Ciononostante tale guerra era comunque soggetta alle regole e ai limiti della legge islamica quali l'inviolabilità della donna, dei bambini, dei vecchi, dei malati e dei monaci. (Carenzi, 2017) Limiti a parte, è a

[33] Con l'espressione panislamismo moderno si intende la tendenza del mondo islamico a creare un'unione tra tutti i popoli musulmani nella speranza di riscatto e rilancio contro la penetrazione politico-culturale europea.

[34] Nella cultura islamica è il principio posto alla base dell'unicità e unità di Dio.

[35] Lo *shirk* è l'attribuzione di un partner ad Allah(cosa o individuo che sia) nella sua Rububiyah e Uluhiyah (Divinità). Esso è il sommo peccato nell'Islam poiché attribuire associati ad Allah è ingiusto. Adorare qualcuno o qualcosa al di fuori di Allah è ingiusto.

[36] Con paganesimo si vuole intendere non il paganesimo in senso stretto bensì l'insieme di atteggiamenti paganeggianti che si contrapponevano all'integrità del mondo islamico. In particolare con il termine pagano si vuole intendere in questo lavoro un atteggiamento laico, allogeno ed edonistico, che richiama a una concezione pratica e non spirituale della vita e che tende all'esaltazione del piacere materiale.

partire da quest'ultima interpretazione di *jihad* quale combattimento di conquista che si dispiegò l'evoluzione concettuale fatta propria dai terroristi jihadisti, i quali fondarono la loro narrativa su tale concetto, seppur stravolgendo, distorcendo e sfigurando i veri precetti dell'Islam. (Carenzi, 2017)

Il fine ultimo dichiarato dai jihadisti è quello di tornare al Califfato classico, paragonabile al Sacro Romano Impero per i cristiani, e la loro dialettica si snoda proprio a partire dall'ideologia della restaurazione dell'età califfale, sebbene materialmente parlando l'obiettivo è ben diverso e si concretizza nel desiderio di despotismo. I militanti islamici infatti portano avanti combattimenti distruttori e ciechi senza alcuna legittimazione ideologica. Il loro operato è assimilabile a quello degli estremismi degli anni '80, di destra o sinistra che siano, che si appellavano a un'ideologia per giustificare le loro azioni ma che poi, nella sostanza, se ne distaccavano completamente. Come nel caso delle Brigate Rosse che giustificavano la violenza armata con l'ideologia comunista, i jihadisti la giustificano con l'ideologia del Profeta, ma in entrambi i casi l'elemento partigiano rimane confinato al *background* e l'espressione della violenza si connota di altri significati.

Questa è quindi l'origine, lo sviluppo concettuale caratterizzante il fenomeno del fondamentalismo islamico, ora dobbiamo capire come è intervenuta la prospettiva globale del jihadismo, quella che ci tocca direttamente poiché diretta a sconvolgere e terrorizzare l'Occidente.

All'inizio il "nemico lontano" occidentale veniva in qualche maniera eluso proprio perché lontano e quindi ritenuto meno pericoloso e prioritario. L'attenzione era puntata sul *dar-al-Islam* e la sua ristrutturazione, per cui *in primis* bisognava eliminare il musulmano deviante rispetto ai precetti del Califfato.

Nei primi anni '90, però, la situazione si ribaltò e in particolare 3 variabili intervenienti fecero sì che il *far enemy* diventasse gerarchicamente rilevante per i jihadisti. In primo luogo l'invasione dell'Afghanistan per mano dell'allora U.R.S.S riunì nel "Paese delle montagne" *mujahidin*[37] da ogni dove con *background* differenti ed essi si riunirono eclissando e ibridando l'ideologia in favore di un'unione di intenti. Inoltre, a partire da quell'episodio, il jihadista quale militante, ormai accomunato agli altri combattenti per il fine della resistenza islamica e non più secondo la sua provenienza geografica, cominciò ad esportare il suo mito anche in altri teatri conflittuali come la

[37] Nel contesto afghano il mujaheddin è il combattente del movimento nazionale islamico durante l'occupazione sovietica e durante il regime de talebani.

Bosnia e la Cecenia[38], per cui la sua dimensione globalizzata si fece sempre più imponente (Carenzi, 2017).

Il secondo elemento propulsore della *globalizzazione del jihad* fu la Guerra del Golfo che accentuò il sentimento anti-americano di molti militanti e accrebbe in seno ai jihadisti un senso di rivalsa sull'Occidente. Infine, la globalizzazione jihadista dipese anche dalle violenze endemiche che si svilupparono in seno a numerosi Paesi musulmani quali l'Algeria e l'Egitto. La lotta per il potere creò aspri scontri tra autorità locali e militanti, tanto che questi ultimi ricusarono in molti casi la lotta armata in patria, ritenuta fallita, per dedicarsi alla conquista di nuovi orizzonti. (Carenzi, 2017)

L'ISIS è la risultante di questo processo evolutivo globalizzante nel senso dell'attenzione che tale organizzazione pone sul *far enemy*; ma il sedicente Stato Islamico non è globalizzato solo nel senso degli obiettivi che colpisce, lo è *ergo et ante omnia* per l'utilizzo dello spazio cibernetico.

L'ISIS è considerata l'organizzazione terroristica più avanguardista di sempre in materia di utilizzo della rete, tanto da essere definita come *cyber caliphate*. La *cyber jihad season* è stata inaugurata da Al-Baghdadi, leader carismatico del sedicente Stato Islamico e sua guida spirituale. Egli diede avvio alla stagione cibernetica dell'organizzazione assodando una ventina di *hackers*, che poi divennero rapidamente gli oltre 3.000 che si contano oggi. (Teti, 2015).

I jihadisti *online* sfruttano la rete per diffondere comunicati di propaganda e coordinare le varie cellule e i molteplici gruppi affiliati, ma anche per fare proselitismo. I social network sono il mezzo più utilizzato, vedasi Twitter, ma gli esperti informatici del *cyber caliphate* si servono anche di canali quali Youtube.

La guerriglia informatica dell'ISIS si incentra sul lavoro svolto dalle "hacking divisions" che combattono una guerra reale nel mondo virtuale. Esse sono formate da *hackers* selezionati in grado di danneggiare i sistemi informatici e le infrastrutture critiche di un Paese. Esempi di obiettivi colpiti dalle *hacking divisions* dell'ISIS sono le violazioni agli account di Twitter, il prelievo di informazioni riservate al Pentagono, l'attacco al Centcom: *United States Central Command* di Tampa e quello al sito web della Malaysia Airlines. (Teti, 2015)

Quello che rende questi *hackers* imbattibili è la loro irrintracciabilità e la loro collocazione geografica: sono ubicati in tutto il pianeta. La loro diffusione planetaria dipende dal fatto che oltre agli *hackers* ufficiali se ne aggiungono altri facenti capo a gruppi simpatizzanti e quindi non

[38] Kepel afferma che nel *milieu* afghano si formò il "salafismo jihadista". Tale dottrina violenta è associata alla seduzione dei musulmani nati in Europa.

formalmente affiliati all'organizzazione madre, ma che contribuiscono ad incrementare la capacità di hackeraggio dell'I.S. Per comprendere appieno la forza distruttrice del *cyber* Stato Islamico basti pensare ai messaggi pubblicati *online* nel caso dell'attacco al CENTCOM, quali ad esempio quello che recitava: "Attenzione soldati americani, stiamo arrivando. Siamo nei vostri computer, guardatevi le spalle.", oppure ai trafugamenti dei documenti top-secret del Pentagono e dei numeri telefonici dei membri del suo personale. (Teti, 2015)

Keystroke logger è il nome del walaware[39] più utilizzato dagli architetti del cyber-califfato. Questo strumento permette di effettuare lo *sniffing* della tastiera, ovvero di intercettare segretamente tutto ciò che viene digitato, senza che l'utente se ne accorga. In questa maniera gli informatici dell'ISIS raccolgono informazioni di ogni genere: da password a numeri di telefono a conversazioni tra esponenti politici di spicco. Questi dati poi vengono diffusi in rete da gruppi che formalmente si interessano ad altro. Per esempio i Tweet pubblicati con gli estremi del personale del Pentagono provenivano da un gruppo denominato Andrew Jackson jihad che appariva come un gruppo di appassionati di musica punk-folk e addirittura connotato geograficamente a Phoenix, come se ci fosse veramente un nucleo di adepti. In realtà gli iscritti a questo gruppo erano simpatizzanti dell'ISIS che si affiancavano ufficiosamente alle *hacking divisions* per aumentare la loro capacità di infiltrazione nella rete. (Teti, 2015)

Il gruppo di *hackers* più attivo dell'IS è il Team System DZ. Esso risulta essere il propulsore della *cyber-war* jihadista. Ne fanno parte *hackers* algerini, yemeniti e giordani e tramite le immagini, i video e i Tweet da loro messi *online* si sono identificati, a volte, anche gli obiettivi nel mirino dell'organizzazione[40]. Ma il Team System DZ non risulta il solo e unico gruppo ufficiale del *cyber-caliphate*. Nella lista stilata dalla compagnia moscovita Group-IB ne comparirebbero altri 2, noti rispettivamente come FallaGa Team e Global islamic caliphate a cui si aggiungono numerosissimi altri nuclei che risultano come affiliati, seppur la paternità della cellula base a volte appare sospetta. (Teti, 2015)

Questa commistione tra ufficiale, ufficioso e rivendicazioni provenienti da ambo le parti rende gli *hackers* e informatici dell'organizzazione sempre più pericolosi e la loro individuazione sempre più difficoltosa. La *cyber-security*, per queste ragioni, è risultata a più riprese fallimentare rispetto alle potenzialità maggiori dell'*Islamic State*.

[39] Il *malaware*, in gergo informatico, indica un software dannoso che mira a disturbare le operazioni svolte da un computer, accedere a sistemi informatici privati e rubare informazioni sensibili.

[40] Brasile, Olanda, Israele, Stati Uniti, Canada, Argentina, Corea del Sud, Danimarca, Iran, Grecia, Norvegia, Repubblica Ceca, Regno Unito, Francia, Thailandia.

Elemento chiave dell'operato degli adepti del cyber califfato è inoltre la tecnica dello *spear phishing* tramite cui essi sono riusciti a perpetrare attacchi a Youtube e non solo. Questa tecnica consiste nella collezione di dati sensibili tramite la creazione di email *fake* che appaiono come sicure ma che in realtà conducono a *malaware*. L'FBI ad esempio ha individuato episodi di *spear phishing* nel caso di e-mail provenienti da *Exploited Children*[41], che in realtà altro non erano che azioni di *cyber-crime*. Insomma, i terroristi *online* sono veri e propri *maîtres* della rete, soprattutto perché sono altamente qualificati e specializzati. Nel computo degli addetti *cyber* troviamo gli esperti di sicurezza informatica, i blogger, gli esperti di comunicazione, coloro che si occupano degli algoritmi di cifratura[42] e i tecnici di reti e sistemi. (Teti, 2015) L'alta specializzazione che contraddistingue i componenti del *cyber-caliphate*, oltre ad essere efficace per gli obiettivi dell'organizzazione risulta anche essere estremamente stimolante e motivante per tutti coloro i quali non si sentono accettati nella società reale e che cercano una forma alternativa di riconoscimento del proprio io.

La cyber-jihad appare come la soluzione alle mancanze della vita reale ed i *cyber-jihadisti* lo sanno. Motivo per cui tra gli esperti del califfato ci sono anche gli addetti alle attività di propaganda e comunicazione tramite strutture *ad hoc*: Al-I'tisaam Media è la scatola nera in cui *web-designer* e registi creano video, contenuti audio e messaggi propagandistici. Il progetto del *cyber-ISIS* si incentra molto sulla parte multimediale e performante oltre che su quella di *hacking*. Su di essa, infatti, il *caliphate*, fonda la sua strategia psicologica e il suo piano organizzativo. La brutalità incarna l'elemento perturbante[43] che spinge la psiche dello spettatore da una parte verso la paura e il terrore ma dall'altra lo indirizza verso un senso di ammirazione per il dolore, quasi di eccitazione. Il filosofo Edmund Burke esprime il concetto di "delightful horror", ovvero dell' "orrendo che affascina" per giustificare questa attitudine della mente umana ad essere attratta dagli aspetti più terrificanti della vita e questo concetto è molto affine alla strategia propagandistica e psicologica dell'ISIS. Gli esperti di comunicazione del *cyber-caliphate* infatti elaborano scientemente contenuti perturbanti, principalmente per terrorizzare il nemico e ingenerare in lui quella costante sensazione di paranoia, trepidazione, inquietudine e angoscia volta a destabilizzare la sua emotività e in

[41] Organizzazione *no-profit* che si occupa dello sfruttamento e degli abusi sui bambini.

[42] Si intende la tecnica di crittografia simmetrica(o a chiave privata) utilizzata tra gli altri dagli *hackers* dell'ISIS; è una tecnica di cifratura in cui la chiave di crittazione è la stessa di decrittazione, per cui l'algoritmo diviene agilmente implementabile permettendo uno scambio rapido e facile tra le parti in possesso della chiave.

[43] È un aggettivo coniato da Freud per esprimere una particolare attitudine del più generico ed ampio sentimento della paura , che si sviluppa quando una cosa viene avvertita allo stesso tempo come familiare ed estranea generando sensazioni di confusione, estraneità ed angoscia.

seguito per impressionare e ipnotizzare l'*audience* tramite l'esaltazione del dolore e della sofferenza, fino ad esaltarlo ed affascinarlo. (Singer, 2012)

Ora che abbiamo fornito un esempio della strutturazione e del tipo di attività svolte dai terroristi "della globalizzazione", nonché evidenziato la loro estrema pericolosità, passiamo ad analizzare una possibile risposta efficace alla lotta al terrorismo.

Intelligence Community per contrastare il cyber-terrorism

Abbiamo visto quanto e come il terrorismo attuale sia figlio dell'era in cui vive. Se la strategia del terrore è cambiata rispetto al passato, dovranno però cambiare anche le strategie di *counter-terrorism*. L'Intelligence, come detto in precedenza, è tradizionalmente un'attività volta alla salvaguardia del territorio statale e alla difesa dei confini della nazione, ma vista e considerata la natura del nuovo terrorismo, è chiaro che essa assuma ormai una rilevanza importante anche nelle relazioni internazionali. Al terrorismo ideologico e politico di un tempo si è infatti sostituito quello *liquido*[44] che caratterizza la società aperta di oggi e con esso i Paesi occidentali prima ritenuti invulnerabili si sono manifestati nelle loro criticità, evidenziando importanti lacune di cooperazione interstatuale in materia penale, tant'è che la legislazione in tale ambito risulta ancora piuttosto frammentaria e autoreferenziale e di conseguenza poco efficace per combattere e annientare terroristi e terrorismi.

Faremo quindi un breve confronto tra le strategie anti-terrorismo impiegate dai principali attori del panorama internazionale: Unione Europea, Stati Uniti e NATO per cogliere le problematiche di coordinazione tra i vari apparati statali e sovrastatali e vedremo in seguito come le carenze individuate necessiterebbero di una Intelligence community più coesa per garantire una maggiore efficacia e una minore penetrabilità.

Partiamo dall'Europa, il cui pilastro fondamentale per combattere il fenomeno terroristico risiede nel motto per cui le minacce non devono diventare conflitto. Logica deduzione è che la prevenzione occupa un posto centrale nelle linee guida della U.E, ragion per cui i fini principali dell'organizzazione sono proprio quello della protezione degli obiettivi potenziali e quello della prevenzione della radicalizzazione e del reclutamento. Ma entriamo più nel dettaglio. Sebbene un'evoluzione in materia di legislazione anti-terrorismo si è verificata a partire dalla creazione dell'EuroJust[45] e dalle modifiche introdotte dal Trattato di Lisbona quali l'introduzione della figura dell'Altro Rappresentante della Politica estera atto a garantire maggiore cooperazione interstatuale in seno all'Unione, la vera svolta della strategia europea sul piano operativo per il contrasto del terrorismo si ha in seguito agli attentati dell'11 Settembre. Da quel momento in poi l'Europa ha

[44] Si faccia riferimento al concetto di "società liquida" di Bauman, il quale teorizzava in cui il soggettivismo esasperato finiva per rendere fragile l'intera società che diveniva quindi fragile e priva di punti di riferimento, dissolvendosi in una sorta di liquidità. Con l'espressione terrorismo liquido si vuole intendere quello operante nella società attuale che risulta come multipolare, multicentrica e senza baricentro solido.

[45] È un agenzia dell'Unione Europea composta da un ufficiale di polizia o un procuratore per ogni Stato membro che insieme formano il "Collegio" dell'organizzazione, il quale è deputato ad eleggere un presidente fra i suoi membri.

cominciato ad operare in modo organico grazie all'adozione di un *Piano d'Azione comune*[46] volto a sconfiggere la minaccia del terrorismo internazionale, poi aggiornato e rivisitato in seguito agli attentati di Madrid e Londra i quali conducono all'elaborazione di un nuovo progetto antiterrorismo articolato in 4 direttrici chiave: prevenzione, protezione, perseguimento e risposta.

Ulteriore incremento all'attività antiterroristica avviene con l'adozione del Piano di Stoccolma[47] che viene posto in essere per disincentivare l'opera di proselitismo, quella di raccolta fondi per fini terroristici e soprattutto che si propugna quale propulsore della collaborazione e l'interdipendenza tra istituzioni e società civile al fine di migliorare la capacità dei singoli stati in materia di difesa e sicurezza contro il terrorismo.

Quello europeo, così come descritto, sembrerebbe essere un modello che punta a una sempre maggiore interazione anche in tema di Intelligence, seppur con delle falle ancora da correggere, ma quello che occorre domandarsi è se la cooperazione in seno all'Unione si manifesta anche oltreoceano, in particolar modo con gli Stati Uniti e con la NATO.

La North Atlantic Treaty Organization attua una strategia di *collective defense*[48]. Questo tipo di approccio, però, presuppone che ci siano dei "mutually shared values", ovvero delle ideologie comuni che formino gli interessi nazionali dei vari stati così da creare un tessuto sociale uniforme e condiviso. Con questa metodologia, è chiaro che la sicurezza viene concepita come indivisibile e quindi da perseguire organicamente da tutti gli stati parte ma il problema che caratterizza questa costruzione teorica è che nella NATO contemporanea, oltre ad una serie di discrepanze meno evidenti ce n'è una su tutte: la spaccatura tra U.S.A e Europa che si fa sempre più significativa e icastica. In un contesto duo-centrico così marcato è difficile pensare che la strategia di *collective defense* possa essere fruttuosa.

Infine ci sono gli Stati Uniti, che nella lotta al terrorismo si dicono aperti al dialogo con stati "alleati e amici" ribadendo l'importanza della collaborazione e della cooperazione per sconfiggere la

[46] Basati su una politica di coesione, i PAC(piani d'azione comune) sono dei programmi della U.E che consentono agli Stati membri di operare congiuntamente nell'ottica di un approccio orientato ai risultati per la realizzazione di un obiettivo prestabilito. Servono per agire collettivamente e in maniera organica laddove ci sono delle minacce o dei problemi individuati come comuni. Il terrorismo ne è un esempio.

[47] È il terzo programma di lavoro quinquennale della U.E in materia di Libertà, Sicurezza e Giustizia in seguito a quelli di Tempere e dell'Aia. Esso, approvato nel 2009, non è vincolante per gli Stati, rappresenta piuttosto un'agenda volta a coordinare le politiche degli Stati membri e il lavoro delle istituzioni europee nella materia di interesse.

[48] Il principio della *collective defense* è enunciato nell'Art. 5 del Trattato di Washington. *Collective defense* significa che un attacco verso un Alleato è da considerarsi come un attacco contro tutti gli Alleati, ragion per cui la risposta deve pervenire globalmente da parte di tutti gli Alleati. L'Art. 5 venne invocato per la prima volta dalla NATO in seguito agli attacchi terroristici dell'11 Settembre contro gli Stati Uniti.

minaccia terroristica ma che, allo stesso tempo, continuano a operare unilateralmente senza pervenire a nessuna forma di dialogo. In particolare, l'Intelligence statunitense, essendo la più avanguardista al mondo relativamente alle tecnologie a disposizione, si pone sempre in una posizione di rilievo e tacita supremazia rispetto alla tematica dell'antiterrorismo. (Aiello, Ardielli, Gagliardi, Michelon, Moro, Toti, 2016)

Avendo analizzato parallelamente i 3 approcci di Unione Europea, NATO e Stati Uniti nonché avendo rapidamente delineato i rapporti che intercorrono tra tali attori, appare evidente che le attività di *counter-terrorism* sono lungi dall'essere organicamente organizzate e che l'idea di una Intelligence community risulti essere ancora piuttosto embrionale.

Ciononostante, forme di cooperazione internazionale in materia di Intelligence e di *law enforcement*[49] sono oggi in essere, seppur scarseggiano trattati applicabili a tali ambiti così come non ce ne sono in merito alla condivisione di informazione tra Stati. La ragione per cui ciò non avviene è insita nelle radici e nella tradizione della società occidentale. La storia democratica dell'Occidente e i principi liberali su cui si è fondato fanno si che l'attività di Intelligence e quella di *law enforcement* non facciano capo a uno stesso organo, in maniera tale da evitare un sistema sulla scia di quelli dittatoriali quale il regime staliniano in cui la polizia di Stato era allo stesso tempo polizia segreta e le libertà costituzionali non rispettate e garantite. (Sipione, 2017)

Nei regimi democratici si violerebbe l'essenza della democrazia se si agisse con un accentramento simile, ragion per cui l'operato dei Servizi di Intelligence è demandato al controllo di organi appositi quali gli Uffici di Controllo. E se questo è quanto avviene in materia di legislazione nazionale, appare ovvio che a livello sovrastatale la problematica del coordinamento Intelligence-forze dell'ordine nonché quella della vicendevolezza relativa allo scambio di informazioni da Stato a Stato risultino difficoltose da portare avanti, sebbene in qualche maniera più avanzate che a livello statale. Importante in tal senso è, ancora una volta, l'attentato alle Torri Gemelle, poiché da quel momento in avanti , lo scambio di informazioni tra gli Stati Uniti e il resto del mondo si è infittito notevolmente e ha creato un meccanismo che nel diritto internazionale verrebbe definito come consuetudinario, ovvero ha generato delle norme che non sono scritte ma che sono ugualmente vincolanti e che vengono di fatto rispettate come se lo fossero a causa della ripetizione continuata nel tempo di un certo comportamento e della convinzione generalizzata che esso sia conforme a diritto. Nella casistica specifica ciò vuol dire che lo scambio di informazioni tra Stati è diventato prassi seppur non c'è nessuna legislazione in materia e che la cooperazione tra Intelligence e servizi

[49] Attività di controllo del rispetto della legge in una determinata area.

di polizia, imprescindibile per combattere il terrorismo multiforme di oggi, è oramai sdoganata a tutti gli effetti. (Sipione, 2017)

La cooperazione internazionale quindi appare come più evoluta ed efficace rispetto agli sviluppi statali. Nel caso della singola nazione gli organi di controllo di servizi di Intelligence e forze dell'ordine sono non solo divisi ma a volte anche in conflitto e questo intacca il funzionamento di entrambi, sia singolarmente che congiuntamente. A livello sovrastatale invece le consuetudini la fanno da padrone e in aggiunta a ciò, nel diritto penale internazionale sono state individuate alcune modalità di cooperazione internazionale utili a sventare la minaccia terroristica, seppur spesso inefficaci poiché caratterizzate da 2 problematiche di base: non sono contenute in un'unica convenzione bensì sparse in convenzioni regionali e soprattutto necessitano, per poter essere applicate, di una legislazione nazionale efficiente ed organica, di cui gli Stati non sono dotati, fatta eccezione per Italia, Austria, Svizzera e Germania.

L'idea di una Intelligence community quindi risulta ancora piuttosto utopica, seppur non sconosciuta, e le mancanze sopra descritte ne bloccano il dispiegamento. Soluzione per sopperire al vuoto legislativo e alla mancanza di raccordo tra i diversi apparati statali risiederebbe nell'incrementare e potenziare il ruolo di **Interpol**: l'ufficio di polizia internazionale per la repressione di attività criminose che si svolgono a livello internazionale ed **Europol:** l'agenzia che si occupa di lotta al crimine nella U.E in prima battuta e nel creare una comunità di analisti di Intelligence prescindente dalla dimensione nazionale in ultima istanza. (Sipione, 2017)

A parte le direzioni che l'Intelligence potrebbe imboccare in un futuro più o meno prossimo, passiamo ora ad occuparci di quelle metodologie di cui essa si è già dotata e di cui si serve per combattere la minaccia terroristica quotidianamente. In particolar modo, analizzando questo lavoro l'aspetto del *cyber-terrorism*, procediamo ad approfondire l'aspetto della Social Media Intelligence (SOCMINT) , branca dei servizi di Intelligence sempre più centrale e saliente.

Capitolo terzo: SOCMINT: strumento di lotta al terrorismo, è realmente efficace?

SOCMINT : che cos'è la social media intelligence: sfide di necessity e legitimacy

Se la dimensione cibernetica rappresenta il teatro in cui va in scena il processo comunicativo di oggi, i social network rappresentano sicuramente il *medium* tramite cui esso viene realizzato.

Come abbiamo visto, la comunicazione in Internet non è controllata ne' filtrata, anzi al contrario, il Web è caratterizzato da lassismo legislativo estremo. Ciò comporta che la mole e la tipologia di informazioni pubblicate *online* sia più che mai ampia e variegata e che le piattaforme di rete vengano usate per gli scopi più disparati. Tra di essi abbiamo evidenziato l'uso della rete per fini terroristici e criminali, *topic* sempre più centrale e rilevante per la sicurezza internazionale.

A tal proposito l'Intelligence si è aggiornata nelle sue tecniche analitiche, cominciando a trascendere la tecnica dello spionaggio e orientandosi sempre più all'utilizzo dei social network quali *agenti infiltrati* nel senso di raccoglitori di informazioni. Questa nuova linea d'azione basata sulla *social media analytics* è conosciuta come SOCMINT: Social Media Intelligence.

Il punto della vicenda consiste nel capire se e come la SOCMINT può realmente essere efficace quale strumento analitico di *counter-terrorism* ed evidenziare d'altro canto i limiti che un'eccessiva fiducia nella tecnologia e nelle sue potenzialità quale mezzo di lotta al terrorismo comporta per un'analisi effettivamente risolutiva e proficua.

I Social Media sono ormai diventati i custodi della vita delle persone, che vi trasferiscono praticamente tutto. Questo rende le piattaforme social un *public space* nel senso di un luogo di scambio come l'agorà nell'antica Grecia e soprattutto rende tale spazio di vitale interesse per i *public bodies*[50], di qualsiasi genere essi siano. Fanno parte di questa categoria anche gli analisti di Intelligence, che tramite la SOCMINT mirano a mantenere ed assicurare la sicurezza pubblica (Troya, 2018).

La Social Media Intelligence presenta sicuramente delle innovazioni rispetto alle tecniche tradizionali di analisi, nonché un valore aggiunto, ma essa si deve misurare anche con due limiti importanti, o meglio sfide note come: Necessity e Legitimacy.

[50]Per *public bodies* si intendono gli enti pubblici , ovvero quei soggetti diversi dallo Stato che esercitano funzioni amministrative e che nel loro insieme costituiscono la pubblica amministrazione.

Prima di introdurre le problematiche relative alle sfide cui la SOCMINT deve far fronte, analizziamo brevemente la marcia in più che tale tecnica analitica fornisce ai servizi di Intelligence.

In primo luogo, le nuove tecnologie distintive della Social Media Intelligence consentono di rilevare la **crowd-sourced information**. Questa pratica consiste nel creare una linea comunicativa diretta tra canali istituzionali quali le forze di polizia e la *crowd* intesa come l'insieme dei cittadini comuni, stabilendo in tal modo un *fil rouge* informativo che permette una collaborazione efficiente e a volte risolutiva in casi di emergenza. Detto in altre parole i social media divengono il *medium* attraverso cui i passive *bystanders* (spettatori) diventano *active citizen journalists* (protagonisti) in grado di fornire e trasmettere notizie utili *dal basso,* così come testimonianze o aiuto di qualsiasi altro genere alle autorità. Un esempio di interrelazione vincente è quella creatasi tramite l'istituzione del *Report by Her Majesty's Inspectorate of Constalbury* riguardante le *riots notes*. Esso è un servizio di messaggistica attivato sul sito Web del West Midlands Police[51] che ha permesso ai cittadini di postare messaggi e interagire con le autorità, facendo loro domande e permettendo così alla polizia di inquadrare la situazione sul campo in tempo reale e allo stesso tempo di diffondere le immagini dei sospettati su larga scala, facilitando il processo di riconoscimento di tali individui e procedendo con molteplici arresti. (Omand, 2012)

Altro elemento di valore della SOCMINT è quello del **research and understanding:** è una pratica analitica consistente nella ricerca basata sui social network al fine di inquadrare e meglio comprendere dei fenomeni di massa. La ricerca avviene tramite l'individuazione e l'utilizzo di soglie, indicatori e standardizzazione di fenomeni quali i percorsi di radicalizzazione. La ricerca consiste nel capire come e perché si formano e si plasmano certe idee e come eventualmente esse possano cambiare. Essa si sostanzia in una parte *online,* che è appunto quella dell'analisi dei contenuti social, accompagnata dall'interazione con la parte *offline*, ovvero l'analisi sociale. Questa è imprescindibile affinché i dati e le informazioni ricavate dalla rete assumano una qualsivoglia rilevanza. Soprattutto in ambito di sicurezza e di *counter-terrorism*, è fondamentale analizzare e capire a fondo il *background* sociale dei terroristi e le motivazioni che li spingono a compiere determinate azioni. Emblematico in tal senso è il lavoro strategico pensato ed operato dalla Military Intelligence (M I) inglese in materia di anti-terrorismo. Gli analisti britannici si concentrano molto sull'aspetto sociologico del terrorismo, analizzano minuziosamente il sostrato sociale ed ideativo dei terroristi e le cause del terrorismo e solo sulla base di un accurato lavoro in questa direzione poi conglobano l'elemento del *social media analytics.* (Omand, 2012)

[51] West Midlands Police è la forza di polizia territoriale responsabile della sorveglianza della contea metropolitana di West Midlands in Inghilterra.

Oltre alle tecniche vantaggiose utilizzate dalla SOCMINT, ci sono poi degli elementi precisi ricavati da esse che aiutano l'Intelligence ad essere più efficiente. In particolare osserviamo la **near real-time situational awareness** che è l'abilità di pervenire a determinate informazioni social e raggrupparle in maniera tale da essere poi in grado di prevedere e descrivere il dispiegamento di un evento. Un caso di questo genere è l'analisi del traffico di Twitter che ha evidenziato un *trend* di utilizzo del social contrassegnante un movimento maggiore in seguito alla diffusione di una notizia da un *mainstream canal* ma una concentrazione di attenzione su quello stesso evento prima che esso venisse ufficialmente riportato. Ciò vuol dire che a volte tramite l'analisi dei contenuti social si potrebbero identificare gli *emerging events* molto più rapidamente che con le tecniche classiche.

L'insight to groups si sostanzia invece nell'analisi dei contenuti social pubblicati da individui, *ergo* account, affiliati a gruppi specifici già "targettizzati" dell'Intelligence o dalle forze dell'ordine. In particolare nella ricerca di *hot topics* nelle conversazioni tra membri e nel caso del terrorismo nell'individuazione del livello di rabbia identificabile nelle discussioni intra-group. Questo strumento è utile per la prevenzione di eventuali azioni violente e allo stesso tempo per una più agile organizzazione della *response* da attuare. Similmente all'approfondimento dei contenuti di gruppi specifici, c'è poi quello che viene definito come ***identification of criminal intent or criminal elements*** nel corso di una specifica inchiesta al fine della prevenzione, in questo caso del crimine ipoteticamente commissibile. L'analisi qui verte sul controllo degli account collegati a un certo individuo ritenuto sospetto o pericoloso tramite la sorveglianza delle sue interazioni social piuttosto che tramite la supervisione delle sue pubblicazioni in linea. (Omand, 2012)

Appare evidente quindi che la SOCMINT è oggi molto importante nel *framework* organizzativo e strutturale dell'Intelligence, ma ciò non toglie che ci siano delle criticità nel suo utilizzo e riguardo al suo *modus operandi* che necessitano di essere analizzate e che riguardano da un lato l'effettiva necessità e l'effettiva contribuzione di determinate azioni alla protezione della società (Necessity) e dall'altro concernono la legalità con cui tali azioni sono portate avanti, ovvero il rispetto del bene comune in tutte le sue parti. (Legitimacy) (Omand, 2012).

Partiamo dalla sfida di **Necessity**. La SOCMINT per essere utilizzata deve dimostrare di essere effettivamente utile al fine del mantenimento e del perseguimento della *public safety* e della *public security*; se così non fosse e le aspettative sulla sua utilità fossero poche o nulle, non ci sarebbe nessuna giustificazione, nessun *argument*, affinché essa possa essere impiegata, in nessun modo. Infatti se la Social Media Intelligence si rivelasse *inefficacious* non solo sarebbe uno spreco di risorse ma causerebbe anche danni collaterali e minerebbe la credibilità dell'Intelligence stessa.

Ma il punto fondamentale consiste nel capire che cosa significa che la SOCMINT deve essere efficace: non si intende la capacità più o meno ampia di collezionare informazioni o segreti bensì l'impatto e il valore aggiunto che essa fornisce ai decisori e quindi al processo di *decision-making*.

I parametri ai quali attenersi al fine di misurare se effettivamente la SOCMINT dà un tributo al processo decisionale ed è quindi aderente al principio di Necessity sono individuabili nelle operazioni di: *data access, processing and analyzing, disseminatio*n *validation and use* dell'informazione. (Omand, 2012)

Il **data access** si riferisce alla mole di dati cui la Social Media Intelligence ha accesso, che è molto ampia. La difficoltà consiste proprio nel discernere i dati rilevanti da quelli irrilevanti. Infatti se l'estrazione dal generale al particolare risulta essere piuttosto sviluppata e aggiornata, nel caso dell'induzione che mira a generalizzare un comportamento la questione si complica. Quando si ha a che fare con *data sets* molto grandi, il rischio di estrapolare informazioni fuorvianti è alto. Il *sample* da creare affinché l'analisi risulti affidabile deve essere rappresentativo e invece spesso è solo molto *large*. Non ci sono molte metodologie che si occupano della rappresentatività del campione.

Questo avviene perché nelle scienze computazionali l'elemento sociologico è lasciato in disparte, per cui si punta sulla quantità e non sulla qualità. Le strategie più utilizzate sono quelle che individuano *campioni di convenienza*[52] o *campionamenti incidentali*, che sono tecniche di facile individuazione e agevole lettura ma poco rivelative. Un esempio di questo genere è fornito sempre dal caso delle London Riots[53]. Quella rivolta fu corroborata da milioni di tweet, tanto che venne creato un progetto *ad hoc* chiamato *Reading the Riots* al fine di identificare i tweet volti all'inneggiamento di attività criminose. Il problema fu che vennero presi in considerazione solamente i tweets contenenti l'hashtag londonriots, il che si rivelò riduttivo e poco sintomatico dell'effettivo utilizzo di Twitter nel mobilitare quella rivolta. Infatti, molti dei sostenitori della mobilitazione non twittarono affatto, o twittarono in altro modo, per cui il campione preso in considerazione non fu calzante ai fini di comprendere la reale incidenza del social network in quell'episodio. E soprattutto molte delle conclusioni elaborate nell'ambito dei risultati del progetto si rivelarono inefficaci, parzialmente inefficaci o addirittura totalmente inutili.

[52] Tale tecnica di campionamento viene effettuata tramite un metodo non probabilistico che non offre la stessa possibilità di essere campionati a tutti gli individui. Alcuni hanno una probabilità maggiore di altri di essere scelti . Il criterio di selezione degli individui dipende da fattori di comodo o praticità , o perché sono disponibili dei volontari, o per ragioni di costo.

[53] Con la locuzione *London Riots* si fa riferimento alle agitazioni popolari che presero piede nella capitale inglese dal 6 al 10 agosto del 2011 e che coinvolsero alcuni dei quartieri periferici della città.

Inoltre, per prendere decisioni in materia di strategie di sicurezza è fondamentale che i *data online* siano implementati da informazioni concernenti i comportamenti al di fuori del Web. Prima per importanza in tal senso è la *rappresentatività demografica*: i social risultano essere utilizzati da quella fascia di popolazione mediamente più giovane, più erudita e più ricca dell'intera società, ragion per cui la realtà *online* non può essere perfettamente aderente a quella reale, anzi spesso crea un'immagine fittizia e distorta dei fatti.

In aggiunta a ciò, all'interno della *online community,* gli *users* sono attivi in maniera differente. Spesso la quasi totalità dell'attività *online* proviene da una cerchia ristretta di utilizzatori delle piattaforme e non da tutti gli iscritti. Questa attitudine è nota come principio paretiano del "vital few": per ogni sito Web identificato, l'80% dei contenuti è pubblicato dal 20% più produttivo degli *users* di quello specifico sito. Appare quindi chiaro che il mondo social è di frequente ingannevole rispetto all'oggettiva e tangibile realtà dei fatti. (Omand, 2012)

Il secondo parametro che la SOCMINT deve rispettare per vincere la sfida di Necessity è quello **dell'elaborazione e dell'analisi dei dati**. Questo *process* avviene in maniera standardizzata tramite approcci computazionali. Ciò significa che la componente umana rappresentata dall'analista di Intelligence è soppiantata dall'automatizzazione dei comportamenti rilevabile tramite algoritmi. Nel dettaglio, l'analisi e l'elaborazione dei dati grezzi collezionati avviene tramite uno specifico approccio noto come *machine learning*[54], il quale tramite alcuni algoritmi è in grado di individuare *patterns*, cioè schemi ricorrenti, e di classificare quindi i dati rilevati.

Una applicazione particolarmente rilevante del *machine learning* è quella della "sentiment analysis" che consiste nella creazione di un algoritmo volto a identificare in un testo specifiche qualità e caratteristiche che esso considera quali statisticamente correlate ad un'emozione o a un sentimento. L'apprendimento automatico (machine learning) offre importanti vantaggi e opportunità di ricerca, ma presenta anche degli aspetti critici e difficilmente sopperibili se non che con l'aiuto della componente analitica umana. Infatti, se da un lato è vero che tale approccio permette la standardizzazione di comportamenti e attitudini, dall'altra non prende in considerazione l'elemento motivazionale di una certa azione ne' analizza il significato che il comportamento identificato può avere.

Il contesto non può mai essere escluso da un'analisi, per quanto evoluta e precisa essa sia. Il linguaggio, che è il *medium* attraverso cui si realizza il processo comunicativo, è strettamente

[54] Il termine *machine learning* è traducibile in italiano come apprendimento automatico ed è una branca dell'intelligenza artificiale che raccoglie un insieme di metodi in varie aree scientifiche. Utilizza metodi statistici per migliorare progressivamente la performance di un algoritmo nell'identificare *pattern* nei dati .

dipendente dal contesto in cui si sviluppa, dalla situazione e dalla cultura. Se il *naturalistic setting* viene ostracizzato dallo studio dei dati, la ricerca e i risultati ottenuti possono portare a disinterpretazioni o interpretazioni fallaci di una determinata fattispecie comportamentale.

Inoltre, il *modus comunicandi* che gli individui utilizzano *online* e quello che invece impiegano al di fuori del Web è dissimile. In rete ci sono norme comportamentali ben differenti da quelle sociali. Non a caso molti studi parlano di "online dishinibition effect", cioè di un modo di interazione *online* più aggressivo, più intenso e più disinibito che nell'interazione *face-to-face.*

Questi elementi nel loro insieme fanno si che il mondo *cyber* plasmi delle sub-culture dei social media, le quali possono creare molteplici difficoltà se non analizzate in maniera dettagliata e tramite un approccio interdisciplinare in cui alla Social Media Intelligence si affianca uno studio sociologico dei fenomeni.

Terzo metro di giudizio per la Necessity della SOCMINT è la **dissemination,** ovvero la diffusione dei dati. Essa deve avvenire in maniera efficiente nel senso che deve pervenire al momento giusto e alle persone giuste in maniera sicura e veloce in modo da essere strategicamente rilevante per il processo di *decision-making.*

Gli ostacoli affinché ciò avvenga però sono molteplici: *in primis* la complessità evidenziata nelle fasi di raccolta e analisi dei dati si riversa anche nella diffusione degli stessi. *In secundis,* la *dissemination* deve essere integrata con i canali *offline* dell'Intelligence quali analisti e ufficiali di polizia che perciò devono essere in grado di trattare le informazioni loro pervenute. Inoltre, i dati collezionati devono essere condivisi e diffusi in maniera sicura. Se la diffusione avvenisse in maniera *unregulated*, la fiducia della gente rispetto alle tecniche della SOCMINT verrebbe compromessa e infine l'informazione che viene ricavata dai social network rimane in qualche misura *network-based,* cioè prescindente dal contesto sociale.

Ultimo parametro per misurare l'ossequio della Social Media Intelligence alla Necessity è rappresentato dalle attività di **validazione e uso dell'informazione**. In questo caso il problema si sostanzia in due variabili principali che possono condurre a un chimerico utilizzo delle notizie estratte dalla rete: l'*observation effect* e il *gaming*.

Andando per ordine, *l'effetto di osservazione* consiste nella variazione comportamentale da parte degli utenti nel caso in cui essi credano di essere sotto controllo. Se tale meccanismo si innesca, automaticamente l'informazione pervenuta dai social network diviene poco efficiente e non descrittiva di un comportamento reale. Se l'utente cambia modo di interagire o non interagisce più

per paura di essere supervisionato, è ovvio che il processo dei dati venga completamente *bouleversé*. Dall'altra parte, gli utenti che si sentono in qualche maniera spiati, possono decidere di giocare, nel senso che invece che smettere di interagire o interagire diversamente, possono optare per la *deception*: imbrogliare e quindi usare deliberatamente i social per confondere e disorientare l'osservatore. Questi due elementi sono chiaramente rappresentativi della vulnerabilità intrinseca alla validazione dell'informazione raccolta grazie alla *social media analytics strategy*.

Ancora una volta, la soluzione per sfruttare al meglio le potenzialità dei metodi statistici e computazioni e ridurne le vulnerabilità, consiste nell'integrare ricerche *offline* al progetto analitico della SOCMINT. In questo modo si avrebbero più elementi a disposizione, la componente contestuale non verrebbe elusa dall'analisi e soprattutto si avrebbe modo di confrontare se e come i comportamenti degli *users online* e *offline* differiscono l'uno dall'altro.

Fino a qui abbiamo messo in luce le criticità strutturali della Social media intelligence in materia di Necessity, ora ci addentriamo nella complessa *challenge* di Legitimacy cui le tecniche di *data-analysis* devono far fronte.

Per essere legittima, la SOCMINT deve subordinarsi al mantenimento dell'equilibrio di tre categorie di *public goods*[55]: la salvaguardia della sicurezza nazionale inclusi l'ordine pubblico e la *public safety*, il diritto dei cittadini alla *rule of law* e il benessere economico e sociale dei cittadini. Questi elementi vanno preservati e garantiti, sebbene i social network abbiano già riscritto la maniera in cui il rispetto di tali principi deve avvenire. In qualche modo le piattaforme *online* hanno modificato e attenuato la natura vincolante di questi beni pubblici (Omand, 2012).

Di seguito analizziamo le ragioni per cui questo abbonimento in favore di Twitter e Facebook si è sviluppato.

Il primo motivo risiede nel fatto che la SOCMINT racchiude nella sua analisi più categorie che si sovrappongono e si intersecano tra loro, ragion per cui tocca delle sfere a volte non formalmente di sua competenza ma che lo divengono *de facto*. Per esempio nel corso di un'indagine, può succedere che la pagina Facebook di un indiziato venga tenuta sotto controllo. Questo è legittimo dal momento che un'azione di questo genere risulta assimilabile e inquadrabile nell'ottica di "autorizzata" da un agente delle forze dell'ordine. Viene in qualche maniera equiparata a

[55] I public goods sono i c.d. beni pubblici, ovvero quei beni che sono caratterizzati da: *assenza di rivalità nel consumo e non escludibilità nel consumo.*

un'operazione condotta sotto mandato. Altro esempio è quello del RIPA 2000[56]. Quel programma ha rappresentato una specie di "autorizzazione a procedere" alle intercettazioni di comunicazione tramite il craccaggio dei codici PIN dei dispositivi targati Black Berry.

La seconda caratteristica che ha cambiato il modo di intendere i limiti della SOCMINT è quella della **generalità**. Se l'analisi dei Social Media avviene senza nominare alcun individuo sospetto ed è volta all'ottenimento di un *output* generale, cioè riguarda la totalità della popolazione social e non si riferisce ad un singolo individuo, allora è legittima. Le analisi condotte sulle reti sociali concernenti la rilevazione di un aumento delle comunicazioni social in una specifica area in un preciso momento storico, per esempio caratterizzato da rivolte pubbliche, non viola la *privacy* degli iscritti.

La **scalability** invece consiste nell'analisi di dati specifici raccolti non facendo un'analisi intrusiva rispetto ad essi, ma sottraendoli dall'insieme delle informazioni disponibili. È una tecnica di estrazione non intrusiva e agilmente perseguibile.

La **flessibilità** si sostanzia nel reindirizzamento di alcune "scraping" technologies[57] verso altre *missions*, cioè obiettivi. Sostanzialmente significa che lo scopo per cui una certa tecnologia utilizzata dalla SOCMINT è stata impiegata può essere facilmente modificato ed aggiustato in base a considerazioni di tipo strategico, senza per questo risultare illegittima.

L'**invisibilità** poi è una forma di sorveglianza coperta che utilizza tecniche specifiche per effettuare l'accesso a dati che gli utilizzatori ritengono privati in base alle impostazioni della *privacy* da loro stessi pensata, ma che invece vengono "spiati".

Infine, la SOCMINT attenua il confine tra sfera pubblica e sfera privata. Proprio per questo, la preoccupazione pubblica riguardo l'utilizzo intrusivo di tecniche di sorveglianza digitale è sempre maggiore. Le informazioni pubblicate in linea sono sempre più in crescita e parallelamente aumentano e si perfezionano in egual maniera anche le capacità di raccolta, recupero, analisi, visualizzazione, distribuzione e trasmissione delle stesse informazioni. (Omand, 2012) Questo rende la preoccupazione a proposito delle capacità intrusive della Social Media Intelligence sempre più ragguardevole. In modo particolare, la paura più grande è quella relativa ai possibili illeciti comportati dalla raccolta massiva di informazioni e gli eventuali danni che essa può comportare.

[56] RIPA è l'acronimo di *Regulation of Investitory Powers Act 2000* ed è un atto del Parlamento del Regno Unito introdotto per disciplinare i poteri dei corpi pubblici in materia di investigazione e sorveglianza, e per coprire (giustificare legalmente) le intercettazioni nelle comunicazioni.

[57] Tecnica per estrarre dati e informazioni dalle pagine dei siti web tramite procedure automatiche.

Alla luce di ciò, è importante strutturare il dibattito sulla *privacy* secondo gli imperativi delle nuove tecnologie e della nuova interrelazione tra pubblico e privato.

Il concetto di *privacy* è fondamentalmente elusivo e lo è ancor di più dal momento che si è adattato ai cambiamenti della società contemporanea. Basti pensare a tutti i contenuti pubblicati e condivisi su Facebook ogni mese: sono contenuti privati nel senso di personali ma vengono volontariamente caricati *online* dagli utilizzatori della rete che così facendo permettono la consultazione di essi a tutti coloro che utilizzano la piattaforma, nel caso di Facebook a tutti gli 845 milioni di iscritti. Questa attività di condivisione non risulta affatto falotica, anzi è il principio fondativo e fondante dei social network. Essi infatti si nutrono e si compongono delle informazioni condivise dagli utilizzatori. Se così non fosse, i social perderebbero il loro carattere di *network.* In questo senso Zuckerberg ha dichiarato che la *privacy* non è più una norma sociale sui social (Omand, 2012).

Il punto cruciale, però, riguarda il fatto che questa trasmissione e diffusione di massa dei dati personali degli individui sia *strictu sensu* consapevole oppure se gli individui non sappiano come potrebbero essere trattate e in che misura le informazioni da loro pubblicate.

Questa possibile mancanza di piena e cosciente comprensione del fenomeno deriva dalla mutabilità del concetto di *privacy* e dalla conseguente difficoltà nel misurare oggettivamente le caratteristiche della stessa. I cittadini che usufruiscono del Web non sono e non possono essere pienamente coscienti delle implicazioni logiche e consequenziali che la messa in linea di certe informazioni può comportare, poiché il sistema delle reti è troppo complesso per poter essere de-secretato.

Ad assicurare una sicurezza in tal senso ed evitare il rischio di una utilizzazione dannosa interviene quindi la legislazione operante in una determinata area: sono le leggi che legittimano o meno un'azione.

In ultima istanza la SOCMINT è legittima o illegittima in base alla legislazione vigente nel territorio in cui agisce, ma data la natura multiforme e sfumata del concetto di *privacy*, anche la legislazione nazionale arranca nel definire e calcolare il moral hazard[58] concernente questa tematica.

[58] Il rischio morale è un concetto introdotto in microeconomia per intendere una forma di opportunismo post-contrattuale che può portare gli individui a perseguire i propri interessi a spese della controparte, confidando nella impossibilità, per quest'ultima , di verificare la presenza di dolo o negligenza. Nel caso specifico della SOCMINT, è difficile definire quanto e come tale attività di Intelligence si svolga in obbedienza dei principi e delle norme sociali vigenti in una certa area e quando invece venga utilizzata per altri scopi.

La legislazione ha lo scopo di misurare l'intrusività della SOCMINT in modo da non intaccare il benessere sociale ed economico dei cittadini. Come abbiamo visto in precedenza però è difficile definire oggettivamente quando, quanto e in che maniera una certa tecnica utilizzata dalla Social Media Intelligence è intrusiva. A tal fine, sono state sviluppate delle teorizzazioni concettuali volte a racchiudere le tecniche analitiche della SOCMINT in 2 macroaree e in maniera da disciplinarne la rispettiva possibilità d'azione su questa base teorica: si tratta di *Socmint non intrusiva* e *Socmint intrusiva*. La distinzione è basata su un elemento specifico che è rappresentato dal controllo tramite consenso dei dati pubblicati *online* dagli utilizzatori da parte degli stessi: se gli *users* controllano l'informazione, la SOCMINT è non-intrusiva, viceversa è intrusiva.

Nel caso della *non-intrusive SOCMINT* essa non dovrebbe utilizzare metodi di ricerca *online* volti a individuare identità bensì l'utilizzo di tale tipologia di SOCMINT dovrebbe essere concepito nello stesso modo che nelle compagnie private, cioè nel quadro delle norme specifiche stabilite in materia di anonimato e protezione dati. Seguendo questo sviluppo concettuale, il *danno* in questo contesto è concepito non come l'intrusione nello spazio di qualcuno ma come la perdita del controllo dell'informazione da parte del possessore della stessa, o meglio l'utilizzo della suddetta informazione per scopi che vanno oltre quelli predefiniti e pre-accettati dall'utente. Onde evitare una deriva simile, le tecniche di collezione e raccolta dati devono essere pubblicizzate e chiare, in maniera tale da non provocare equivoci, incomprensioni e eventuali abusi di potere.

L'altro lato della medaglia invece è quello della *SOCMINT intrusiva*. Molti Paesi hanno già un quadro normativo per l'utilizzo di questo tipo di Intelligence in materia, prima fra tutte, di sicurezza nazionale e prevenzione del crimine. Ciò che è importante nel caso dell'analisi dei dati intrusiva, è che ci sia una accettazione pubblica e quindi una convinzione generalizzata che la sorveglianza statale e gli accordi relativi al dispiegamento dei mezzi per metterla in atto siano in conformità con i principi etici riconosciuti in seno alla società in questione. (Omand, 2012)

Concludendo il discorso legato alle sfide gemelle di Necessity e Legitimacy si può dire che la SOCMINT deve, nel caso della Necessità, provvedere a dare vita a una vera e propria *scienza delle reti sociali* che si componga della parte *online* dell'analisi dei Big Data ma che veda anche una parte *offline* di analisi volta a comprendere e contestualizzare i comportamenti degli individui sulla base dello studio di discipline quali l'antropologia, la psicologia e la scienza politica.

Per quando concerne invece la Legittimità, la sfida può essere vinta solo tramite una comprensione e una conseguente accettazione *in toto* del fenomeno da parte della società. A tal fine l'intervento governativo è imprescindibile affinché si crei una cultura della SOCMINT e affinché si adotti un

approccio applicativo di essa conforme ai diritti umani nonché in ossequio dei principi di accountability, necessity e proportionality. [59]

[59]Principi chiave del GDPR, ovvero il regolamento europeo in materia di protezione dei dati personali(general data protection regulation). Per approfondire si consulti: https://www.laleggepertutti.it/231903_gdpr-principi-fondamentali

Ostacolo della SOCMINT: signal-to-noise ratio

Fin qui abbiamo elencato e analizzato le barriere teoriche che la Social Media Intelligence deve superare per essere a tutti gli effetti riconosciuta quale branca ufficiale dei servizi di Intelligence (Necessity e Legitimacy), ora invece la prospettiva analitica che adotteremo sarà relativa all'inquadramento e alla spiegazione del principale ostacolo pratico cui la SOCMINT deve rispondere al fine di essere realmente efficace: il **signal-to-noise ratio** (Mele, Faini, America, 2016).

La raccolta informativa rappresenta da sempre il principale strumento analitico per le agenzie di Intelligence, nonché il lavoro più meticoloso e delicato da compiere. La mole di informazioni che i servizi si trovano a dover maneggiare è da sempre ampia e variegata, per cui difficile da trattare.

Con la rivoluzione digitale e quindi l'avvento dei mezzi di comunicazione di massa e la successiva entrata in gioco dei social network, la dimensione informativa e la struttura comunicazionale sono state del tutto stravolte nel loro fondamento concettuale e con esse è cambiata anche l'attività di raccolta e collezione di Informazioni da parte degli analisti di Intelligence.

La SOCMINT è stata la risposta che essi hanno dato alla rivoluzione *network-based*, ma essendo una branca in fase di costruzione e di recente scoperta, essa presenta delle falle di base che devono essere corrette. Prima fra tutte quella del signal-to-noise ratio sopra menzionata. Con tale espressione, che in italiano si traduce come *rapporto tra segnale e rumore*, si identifica la difficoltà nel distinguere le informazione realmente rilevanti dall'insieme infinito di scambi comunicazionali (rumore) che avvengono sulle piattaforme di Internet. La bravura degli analisti risiede proprio nella capacità di discernere le tematiche di interesse da quelle inutili o distrattorie. Nel social infatti ci sono varie informazioni che, nel gergo sei servizi segreti, vengono classificate come: falsi positivi, falsi negativi e disinformazione.

Prendiamo come esempio il fenomeno del terrorismo che è quello che ci interessa. Se lo Stato Islamico ha 1 milione di simpatizzanti sui Social Network, ciò non vuol dire che tutti questi individui passeranno poi a compiere l'azione concreta e quindi a fare un attentato.

In questo caso, tutti coloro che potrebbero essere ma non sono effettivi combattenti sono elementi identificati quali casi di **falsi positivi**. All'opposto, i veri attentatori potrebbero avere tutto l'interesse a non scrivere nulla sui social per non destare sospetti, e quindi potrebbero completamente inutilizzare la comunicazione *online* per pianificare l'attacco. Qui si parla allora di

falso negativo: tutti quei casi di interesse che non risultano visibili tramite l'analisi dei contenuti pubblicati in rete.

I terroristi inoltre per fronteggiare l'avversario devono cercare di anticiparne la mossa e depistarlo. Per questa ragione spesso essi alimentano in rete un chiacchiericcio inutile e fittizio volto a disorientare e fuorviare il nemico e questo è il fenomeno della **disinformazione**. (Mele, Faini, America, 2016)

Il "franchising" del Califfato (Caracciolo, 2016) è stato utilizzato per la questione Libia *in primis*. Gli adepti dell'ISIS veicolavano messaggi *online* relativi alla conquista di tutto il territorio libico, ma nella sostanza non era così. I video delle decapitazioni sommarie di ostaggi dell'organizzazione incrementavano la risonanza del messaggio e nello spettatore che apprendeva la notizia non si insinuava nemmeno il minimo dubbio che potesse trattarsi di una montatura *ad hoc*, poiché egli rimaneva attonito e terrorizzato da una simile propaganda. La violenza era ed è tutt'ora l'arma che i terroristi usano per rendere credibile ciò che dicono. Le atrocità aiutano a disinformare (Chiari, 2015).

Il problema del basso *signal-to-noise-ratio* è importante in questa disamina perché è strettamente rilevante in materia di terrorismo. Infatti se sugli eventi di massa in cui la partecipazione è cospicua la vulnerabilità del Web appare meno evidente perché il margine d'errore è più ristretto, viceversa quando si tratta di eventi riguardanti una cerchia ristretta di individui come appunto gli attentati, la prevedibilità dell'evento sulla base delle informazioni riscontrate grazie all'impiego della SOCMINT è sicuramente molto difficile.

Per sopperire alle carenze dei Big Data quali indicatori unici ed assoluti degli *expected events* bisogna ritemprare la logica degli algoritmi con il c.d metodo "human-sized".

L'analisi dei Big Data da sola non basta: l'interazione con le scienze sociali : "human-sized"

Le informazioni di bassa qualità devono essere trasformate in informazioni di valore. L'implemento qualitativo può avvenire solo tramite una corroborazione e un'integrazione perpetua tra SOCMINT e HUMINT. Per sfruttare a pieno le capacità della Social Media Intelligence occorre trasformare i dati collezionati grazie alle reti in elementi di interesse.

Sempre rimanendo nel campo delle azioni terroristiche è di facile comprensione che se un social network permette di reperire informazioni riguardanti il *modus comunicandi* di un presunto terrorista, non consente di tracciarne un profilo. Con l'ausilio delle piattaforme *online* si possono carpire elementi importanti in merito alla rete interattiva che il soggetto ha sviluppato, tramite le date e i luoghi di connessione si possono tracciare i suoi spostamenti e conseguentemente fare un quadro delle sue abitudini. Ma a tutto ciò va integrata l'attività di *profiling* e contestualizzazione, imprescindibile nel *case study* del terrorismo. La HUMINT è chiamata a fare proprio questo. Gli analisti hanno il compito di studiare il percorso dell'individuo sospetto al fine di metterne in luce eventuali elementi di interesse che possono essere precedenti penali piuttosto che un *background* familiare poco lineare. In tal senso c'è bisogno di un *continuum* analitico. La sinergia delle fonti "human-sized" e di quelle *online* permette di delineare il quadro completo di una fattispecie.

In quest'ottica va da sé che le diverse agenzie di Intelligence non sono in contrapposizione l'una con l'altra ma che, al contrario, si alimentano a vicenda nello scopo di raggiungere un obiettivo comune. Se la HUMINT operasse in solitaria senza fare ricorso alla "datizzazione" , il lasso di tempo che intercorrebbe tra la fase di collezionamento dei dati e la fase operativa sarebbe elefantiaco. Allo stesso modo se la SOCMINT si ponesse in una prospettiva di sovraordinazione rispetto alla parte umana di analisi, essa resterebbe uno strumento efficace per creare mappe interattive e in tempo reale ma che sarebbe in grado di agire solamente tramite metodo deduttivo e non anche induttivo.

Intelligence italiana VS Intelligence americana: un differente utilizzo della SOCMINT(HUMINT e SIGINT)

Il dibattito riguardante l'utilizzo più o meno intercorrelato delle diverse fonti di Intelligence è centrale oggi da un punto di vista strategico, politico, economico e tecnologico.

In prima linea quali difensori della SOCMINT quale strumento di assoluta efficacia troviamo gli Stati Uniti. Non è una sorpresa se si pensa alla capacità informatica di cui possono usufruire. Gli *States* infatti rappresentano il Paese globalizzato per eccellenza e logica conseguenza di questo assetto sociale è la concezione dei mezzi di comunicazione e delle nuove tecnologie quali elementi provvidenziali al fine della floridità, dello sviluppo e della dimensione avanguardista della società. In questa direzione negli U.S.A si è sviluppata la corrente *mainstream* in difesa della Social Media Intelligence. Tra i sostenitori più convinti ed entusiasti di questa metodologia analitica c'è Jane Harnan, Presidente del Wilson Center for International Scholars. Secondo lei, i tradizionali metodi di raccolta impiegati dalla HUMINT sono di gran lunga meno efficaci della collezione dei dati che è possibile operare tramite l'analisi delle piattaforme *online*. (Mele, Faini, America, 2016)

Nel caso delle vicende russo-ucraine ha infatti dichiarato che :"per seguire le vicende in Ucraina alla CIA non serve una fonte all'interno del Ministero dell'agricoltura russo.", poiché il rendiconto migliore si ha grazie ai social network. (Mele, Faini, America, 2016).

A conferma del fatto che questa linea di pensiero sia *mainstream* in America basta guardare la struttura organizzativa dei servizi di Intelligence statunitensi: la divisione operativa non avviene per aree geografiche, bensì per settori. Per cui la HUMINT opera distintamente dalla SOCMINT comportando un'interazione praticamente nulla tra le due attività. L'interoperatività è sfavorita da una simile concezione strutturale tanto che John O.Brennan[60], ha proposto una riforma affinché possano essere introdotti all'interno della CIA degli uffici in cui le diverse discipline possano convivere e operare fianco a fianco (Omand, 2012).

Sul principio di operatività congiunta invece si basa la struttura dei servizi italiani. Nel nostro Paese l'Intelligence appare più coesa, tanto che la divisione operativa è effettuata secondo aree geografiche e non tramite settore disciplinare. In Italia abbiamo l'AISE: agenzia informazioni e sicurezza esterna e l'AISI: agenzia informazioni sicurezza interna.

Lungi dal fornire un'analisi comparata al fine di emettere un giudizio di valore sul merito dell'analisi condotta dai servizi statunitensi e quelli italiani , in questa disamina si vuole solamente

[60] Direttore della Central Intelligence Agency (CIA) dall'8 marzo 2013 al 20 gennaio 2017.

mettere in luce la divergenza sostanziale tra il *modus operandi* SOCMINT-based, più spesso utilizzato negli Stati Uniti e quello SOCMINT_HUMINT based, proprio delle nostre agenzie di Intelligence. Tale differenza consiste nella fase di verifica delle informazioni: nel caso di in utilizzo isolato della SOCMINT la disseminazione dell'informazione, ovvero la sua trasmissione ai *decision-makers*, appare come priva di verifica *ex post*: l'operatore di Intelligence non interviene a "sgrezzare" i Big Data e quindi non adopera un metodo epagogico volto a contestualizzare una determinata situazione, per cui l'analisi conclusiva è la risultante della sola attività di estrazione e delle sole tecniche inferenziali condotte sui social per emettere macrocampioni di studio.

Al contrario, nel caso dell'approccio interoperativo SOCMINT-HUMINT si effettua un accertamento posteriore alla collezione informativa pervenuta dai social network. Lo scopo dell'intervento della componente umana tra la fase analitica e quella di disseminazione è di raffinare l'informazione ottenuta dalla rete, innalzandone il livello qualitativo tramite un meccanismo di filtraggio *human-oriented*.

In conclusione, la SOCMINT rappresenta una novità intelligente, ma essa ha ancora bisogno di essere inquadrata e concepita in maniera organica e condivisa. Si è visto come essa sia più efficace in ambiti macro e meno in contesti micro e come ci siano delle questioni etiche che ne frenano il dispiegamento incondizionato quali la *privacy* e il benessere socioeconomico dei cittadini. Si è poi accennato alle principali utilizzazioni che vengono fatte di tale branca dell'Intelligence, ponendo il *focus* sull'approccio italiano e sul metodo statunitense, al fine di indicarne i rispettivi orientamenti portanti.

Conclusioni

La Network Society ha traslato la società in una dimensione globalizzata. I meccanismi che governano un sistema così concepito sono senza dubbio legati alle nuove tecnologie, le quali rappresentano la chiave di volta della società aperta ma anche uno strumento pericoloso. Infatti, a partire dalle nuove tecnologie si sviluppano minacce prima impensabili e impossibili da realizzare, prima fra tutte il cyber-terrorismo. Sulla scia di questo fenomeno, unito a quello del cyber-crime, l'Intelligence ha dovuto fare un grande lavoro di aggiornamento e ha dovuto ridisegnare le sue logiche analitiche e applicative. Non esenti da critiche, i servizi segreti sono oggi in fase di ricostruzione, seppur agli occhi di alcuni appaiono come devitalizzati e sopraffatti dalle capacità distruttive del Web. Al fine di mostrare le vulnerabilità che debbono essere vinte, *Wikileaks* e la figura di Assange sono emblematici, così come è significativo il caso dello Stato Islamico nella sua configurazione *cyber-oriented*.

D'altro canto, l'Intelligence non ha solo subito la rivoluzione digitale e seppur ancora in fase di definizione, i servizi sono sulla strada di una riforma strutturale. Certo è che gli ostacoli a cui essi devono far fronte sono molteplici e gli interessi in gioco da rispettare altrettanti: la concezione ancora territoriale dell'attività di Intelligence, la difficoltosa e porosa integrazione sovrastatale , la spaccatura sempre più netta all'interno della NATO rendono il processo di ristrutturazione e ricognizione dei servizi ancora *in fieri* e alquanto embrionale. La dimensione globalizzata non ha ancora fatto presa sull'attività di difesa, ancora incentrata e concepita entro i confini statali.

In aggiunta a ciò, quei passi che sono stati fatti in materia di tecniche analitiche aggiornate in chiave social media-oriented, risultano piuttosto contraddittori e godono di una legittimazione ancora parziale. La pretesa universalistica della SOCMINT appare come utopica sia da un punto di vista di efficacia sia nell'ottica del rispetto dei principi vigenti nel contesto democratico in cui si sviluppa.

Le sfide da vincere per l'Intelligence moderna sono tante e complesse: cyber terrorismo, carenze struttural-organizzative, contesto sociale e diritti, quadro politico internazionale frammentario e poco organico.

La cyber euforia che ha contraddistinto i primi decenni successivi alla nascita dell'era digitale ha lasciato spazio a una presa di coscienza e un successivo ridimensionamento di giubilo. Il *restyling* dell'Intelligence deve ancora fare molta strada.

Bibliografia:

Testi:

Campagnoli, M.N. (2017). *I nuovi volti del terrore dal terrorismo islamico al cyber terrorismo: fenomenologia di una perturbante forma di violenza*. Cendon/Book. Key Editore Srl.

Colonna Vilasi, A. (2011). *Manuale d'Intelligence*. Reggio Calabria: Città del sole edizioni s.a.s.

Giannuli, A. (2018). *Come i servizi segreti stanno cambiando il mondo: le strutture e le tecniche di nuovissima generazione al servizio delle guerre tradizionali, economiche, cognitive, informatiche.* Casa editrice Ponte alle Grazie.

Giannuli, A.(2012). *Come i servizi segreti usano i media*. Pioltello (Milano): Adriano Salani Editore S.p.A

Troya, A. (2018). *Social Media Intelligence: I movimenti islamici sulla rete: la propaganda islamista e le ragioni nel Web*. Paperback edizioni.

Articoli online:

Acquaviva, M. (2018) Gdpr: principi fondamentali. *La legge per tutti, informazione e consulenza legale.* Consultabile al link: https://www.laleggepertutti.it/231903_gdpr-principi-fondamentali

Aiello, A., Ardielli, N., Gagliardi, V., Michelon, M., Moro, A., Toti, E. Confronto strategie di sicurezza: UE-USA-NATO. *Centro diritti umani*, p. 1-71. Consultabile al link: http://unipd-centrodirittiumani.it/public/docs/confrontostrategie.pdf

Allan, S. (2007). Citizen Journalism and the Rise of "Mass self-Communication": Reporting the London bombings. *Global Media Journal, Australian edition.* p. 1-10. Consultabile al link: https://www.hca.westernsydney.edu.au/sites/wp_gmjau/archive/iss1_2007/pdf/HC_FINAL_Stuart%20Allan.pdf

Bastiani, D. (2012). Terrorismo e Media: la comunicazione del terrore. *Informazioni della Difesa*. 2/12. p. 36-43.Consultabile al link: https://www.difesa.it/InformazioniDellaDifesa/periodico/periodico_2012/Documents/R2_2012/36_43_R2_2012.pdf

Boria, E. (2015). Intelligence e Geopolitica: incroci plurimi, oggi come ieri . *Gnosis:Rivista italiana di Intelligence* ,p. 38-46. Consultabile al link: http://gnosis.aisi.gov.it/gnosis/Rivista45.nsf/ServNavig/45-29.pdf/$File/45-29.pdf?OpenElement

Brando, G. (2018). Introduzione alla Cyber Intelligence. *ICTSecuritymagazine. com.* (10/04/2018). Consultabile al link: https://www.ictsecuritymagazine.com/articoli/introduzione-alla-cyber-intelligence/

Buoncompagni, G. (2016). Violenza contemporanea e cyber terrorismo. p.1-8. Consultabile al link: https://www.researchgate.net/publication/320799113_Violenza_contemporanea_e_cyberterrorismo

Caforio, A. (2018). Cyber Threat Intelligence: cos'è e come aiuta la sicurezza aziendale. *Cybersecurity360.it.* Consultabile al link: https://www.cybersecurity360.it/cultura-cyber/cyber-threat-intelligence-cose-e-come-aiuta-la-sicurezza-aziendale/

Carenzi, S. (2017). L'evoluzione ideologica e operativa del jihadismo globale. p.1-18. *Sicurezzanazionale.gov.* (05/09/2017). Consultabile al link: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/09/evoluzione-jihadismo-Carenzi.pdf

Chiari, R. (2015). "Italia e UE in balia dell'inganno mediatico dell'ISIS.", *L'informatore.* Consultabile al link:http://www.informatore.eu/articolo.php?title=caracciolo-italia-e-ue-in-balia-dell-inganno-mediatico-di-isis

Digital Guide (2018). *Ionos.it* Consultabile al link: https://www.ionos.it/digitalguide/server/know-how/che-cose-il-protocollo-internet-definizione-di-ip-co/

Gagliardi , C. (2019). *Villaggio globale*, in Franco LEVER - Pier Cesare RIVOLTELLA - Adriano ZANACCHI (edd.), *La comunicazione. Dizionario di scienze e tecniche*, www.lacomunicazione.it (07/06/2019). Consultabile al link: https://www.lacomunicazione.it/voce/villaggio-globale/

Gioia, A. (2018). La network society di Manuel Castells, iperconnessa e ipercomplessa. *Periodicodaily.com.* (08/02/18). Consultabile al link:https://www.periodicodaily.com/la-network-society-manuel-castells-iperconnessa-ipercomplessa/

Guida, S. (2019). Rischi e "instabilità" tecnologici nell'edizione 2019 del Global Risks Report del World Economic Forum. Parte 1. *ICT Securitymagazine.com* (29/01/19). Consultabile al link: https://www.ictsecuritymagazine.com/articoli/rischi-e-instabilita-tecnologici-nelledizione-2019-del-global-risks-report-del-world-economic-forum-parte-1/

Killelea, E. (2017). Wikileaks pubblica dei documenti della CIA: ecco tutto quello che c'è da sapere. *RollingStone.it.* (13/03/2017). Consulabile al link: https://www.rollingstone.it/rolling-affairs/news-affairs/wikileaks-pubblica-dei-documenti-della-cia-ecco-tutto-quello-che-ce-da-sapere/356082/

Marro, E. (2016). Inspire, il magazine del terrorismo islamico che ispira i "lupi solitari". *Il Sole 24 ore*. Consultabile al link: https://www.ilsole24ore.com/art/mondo/2016-07-19/inspire-magazine-terrorismo-islamico-che-ispira-lupi-solitari-164036.shtml?uuid=ADrZr4u

Mele, S., Faini, M., America, C. (2016). Social media intelligence e sicurezza nazionale. La raccolta informativa sui social media. *Sistema di informazione per la sicurezza della Repubblica* ,p. 1-

7.10/02/2016. Consultabile al link:https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/02/Socmint-Mele-Faini-America.pdf

Nye, J. (2004).Soft Power: The Means to Success in World Politics.p.1-28. Consultabile al link: https://www.belfercenter.org/sites/default/files/legacy/files/joe_nye_wielding_soft_power.pdf

Omand, D. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence & National Security* , p. 801-823. Consultabile al link: https://www.tandfonline.com/doi/abs/10.1080/02684527.2012.716965

Rapporto UNODC: United Nations Office on Drugs and Crime. (2012). The use of Internet for terrorist purposes, p. 3-30. Consultabile al link: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Singer, P. (2012). The Cyberterror Boygeman. *Brookings* . Consultabile al link: https://www.brookings.edu/articles/the-cyber-terror-bogeyman/

Sipione, L. (2017). Dal terrorismo politico alle nuove forme di terrorismo globale: strumenti di conoscenza e di contrasto in ambito nazionale ed europeo. SNA, Scuola Nazionale dell'Amministrazione. *culturaprofessionale.interno.gov.* p.2-43. Consultabile al link: http://culturaprofessionale.interno.gov.it/FILES/docs/1260/TESTO%20INTEGRALE%20Sipione.pdf

Swisstopo (ufficio federale di topografia per la Svizzera) . *Geoinformazione e geodati*. Consultabile al link: https://www.swisstopo.admin.ch/it/conoscenze-fatti/geoinformazione.html

Teti, A. (2015). L'arma dell'ISIS: Cyber Caliphate per combattere la cyberwar.GNOSIS:*Rivista Italiana di Intelligence* , p.75-86. Consultabile al link: http://gnosis.aisi.gov.it/gnosis/Rivista43.nsf/ServNavig/43-38.pdf/$File/43-38.pdf?OpenElement

Siti:

Difesa.it

Abstract

This thesis analyses three different themes that are linked between them due to the macrophenomenon represented by the naissance of the Netwotk Society, that is the starting point from which this speech is articulated.

Before of explaining what Network Society is and how it affected the contemporary world, we have to introduce the three aspects dealt in this work, that are, in order: the change of the Intelligence services and of the threats they have to fight, the cyber-terrorism menace, its implications and its way of acting and finally the introduction of SOCMINT technique among those already avalaible to the secret services.

First of all, we have to move from the explanation of the concept of *network society*: this is an expression coined by the sociologist Manuel Castells. He describes it as:" a society whose social structure is made up of networks powered by micro-electonics-based information and communication technologies."

What Castells strongly underlines is not the existance of the Social Networks, that he says have always been actual rather than merely possible, but he focuses on the use of the ICTs.

The *information and communication technologies* help to create and sustain far-flungs networks in which new kinds of social relationships are created. People were born as "species being" , to use the evocative words of Marx: it means individuals are essentially social beings rather than human beings, whose primary necessity is to communicate with each other. ICT's offer the possibility to do it more quickly, rapidly and effettively so that the *appeal* they have on most people is quite a primordial urge.

This is a key point in this thesis because the new threats and the consequent new nature of the Intelligence forces arise from the new *network-based* way of living and interacting. The digital revolution not only changed the way of intending technology, it also shaped a new ontology- both in civil and network society- that resulted in a digital being. What Robert Putnamm called "social capital" is growing dying. Social engagement is reducing in favour of digital engagement.

Before the globalization of the information took place, the flux of communication between people was characterised by a 1:1 ratio: for one sender there was one receiver. After the rise of the *Internet era*, communication process turned toward the so said **mass self communication.** The key principles of this form of communication are: an interactive commmunication that "connect local

and global in chosen time" , a horizontal structure of the messages, while before of it the dynamic was a top-down one and last not least, a potential global audience included in the distribution of the information. (Allan, 2007)

This means the mass media have pluralised the information. But the crucial point is that this phenomenon of inclusion is only apparent because contrary to what is known, the new technologies contribute to create exclusion and to emphasize differences. The massification of the information is unevenly distributed, indeed it concerns only certain individuals and certain social classes. This net stratification of society created by the netwoks led to increasingly clivages within the same. This phenomenon is known as "digital gap" : on one side there are people who have access to the network and on the other the excluded, totally or partially, from the online communication process.

As a consequence of this unfair dissemination of the information, societies have always more resulted in split, cracked and devoid of a social tissue and this led to the emergence of new phenomenons such as cyber-terrorism. In fact, many people espoused the cause of terrorism because of their lack of recognition at the interiour of their place of belonging. These individuals see the cyber dimension as an escape room, a new dimension in which they have the chance of reaffirming their personality, their strenght and their value. It is clear that the psychological element is dominant and central in the case of terrorism. Legitimacy is given by the sentiment of need that adepts feel. Cyber-space is useful to create this feeling. Radicalization and brain-washing processes are prevalently beared by the online strategy.

Internet is nowadays fundamental for the strategic analysis and actions made by the cyber-terrorists. It is used by them both as a *tool* and as a *target*. As a tool, the Internet space is exploited as a vector for: activities of propaganda, fund-raising, training and planning, all made on the Web. The goal of terrorists in this case is to use the cyber-space to recruit new followers and new funds in order to achieve their goals. The other way around, using the online platforms as a target means that terrorists exploit the vulnerabilities of the Web in order to create a damage to the critical infrastructures of a territory. The techniques covered by the target oriented strategy are the execution and the cyber-attacks.

If network society resulted in cyber-terrorism on one hand, on the other hand it also meant the complete translation of the Intelligence services toward a cyber-oriented vision.

The actions of espionage are not performed anymore and the secret agents are somewhat cliché and old-fashion. They have left space to new methods of collection and analysis of the information, especially to Internet-oriented approches. The aspect we want to analyse in this work is that of the

SOCMINT: social media intelligence, that represents one of the most cutting-edge techniques Intelligence services have in their packet. This consists in collecting Big Data through the analysis of the communication that takes place on the social platforms such as Twitter and Facebook.

It is a great tool to extrapolate large samples but the great difficulty linked to this method is that the representativity of the sample is not guaranteed. In fact, statistics does not provide useful information on the social context or about the background of an individual, it only gives to the server evidence of the conversations that a certain individual had on the affected platform rather than posts he made or groups he joined to.

In order to assure a great result, SOCMINT should be paired to the human component. In fact, analysts can not be set aside, they are still fundamental for the success of the Intelligence activities.

The themes listed above are those relevant in this work, now we go to see more in detail what the three chapters of the thesis treat.

In the first one it is explained the reason that gave birth to the Netwotk Society and the consequences this new conception of life generated. In particular, the focus is posed on the sociological change people made in order to get with the times. Subsequently it is introduced a paragraph concerning the new Intelligence that arised from the rise of this new *information order* and finally it is proposed the case study of Wikileaks'incidents in order to show the weakness of the secret services, in this case of the American ones: the CIA (central Intelligence Agency) , the most updated in terms of both money and tools among the global forces of Intelligence. Assange's platform published the biggest confidential documents' leak ever, known under the name of "Vault 7" that provoked a collapse of CIA for a while. It is emblematic for the purpose of showing as Internet & Co. rules the world.

Proceeding in order, the first point is to understand why Network Society provoked a similar upheaval: it is fundamental to intend it as a product of the globalization. This term describes the interdepence of the world's cultures, economies, socities and populations, brought about by cross-border trade in services and goods, investments, people, technologies and information. The key word to understand this growing connection is **partnership**. Nowadays every thing is based on bilateral agreements or similar arrangements, not only economically but also concerning other topics.

Politically talking, for instance, the art of make politics drastically became more a question of personal interest and affair rather than an activity made for the public good.

The dimension politics assumed is not linked to an area anymore, it is rather dependent on the interest of the élites. Communication and information dynamics work the same way. Platforms, channels and Websites are the *arena* in which exponents of the new establishment perform their strategies. The new ruling class is formed by the multinational entreprises, by the groups of interest and by non-profit organizations. These actors were unknown before the rise of the digital-age, but they became the absolute protagonists after it appeared.

On the other side, the Web is also used by other actors known as cyber-terrorists. They represent one of the greatest vulnerabilities of the globalised world and this is the topic we face in the second chapter.

The second part is about terrorism and its new cyber declination. Firsly, we trace the path of the phenomenon since its origins to the modernity, then we analyse the different uses terrorists make of the Web, thirdly we put into pratice what we explained about the use of the cyber-space through the case study of the ISIS terrorist group and finally we introduce an overview of the counter-terrorism activities'situation at the present times.

What is underlined in this chapter is the need of the Intelligence to be updated in its structure in order to win and to prevent terrorist attacks. In particular, the Intelligence community as it is now conceived, as a national activity, is extremely vulnerable and weak if compared with the liquid terrorism we know. Responses to terrorism are no longer benchmarks-based on geography and due to this , it is essential to connect the activities of the different actors who have voice on the matter, specifically: NATO, European Union and United States.

The third chapter and the conclusive one is indeed centered on the SOCMINT strategy, considered as a great response to the new transnational form of terrorism. First and foremost Social Media Intelligence is introduced in its key points, it is analysed in its core and then the attention is posed on certain problems this techniques could lead to if used singularly. Especially the signal-to-npise-ratio difficulty is taken into account. This expressions means that on the network there is a large amount of information and this makes difficult for computational methods to separate the relevant Data and the unuseful ones. As a result of this, the following paragraph proposes the "human-sized" approach, in other terms the combination of social media analytics to the analysts' contribution, as an efficient response to the signal-to-noise-ratio. Only through the collaboration

and coordination between the online and the offline, a true picture of the specific situation is possible. To conclude, it is proposed a comparison between the Italian Intelligence and the American Intelligence with regard to the use of SOCMINT. United States' strategy gives priority to the analysis of Big Data while Italian Services combine SOCMINT to HUMINT sources.

In conclusion, this work is made firstly for giving a general idea of the revolutionary extent provoked by the rise of the Network Society. The objective here is not only to show how the digital age introduced the *mass self communication* but it is above all a work aimed at understanding how the ICT's are affecting people in their ontology, how globalization both economic and technological is shaping a new world in which real spaces are overwhelmed by the pluralism that arises from the networks.

Furthermore, this thesis seeks to introduce the cyber-terrorism in order to highlight its key points, given the breadth of the phenomenon. Attempts have been made here in order to orient the reader to a better understanding of this *affair*, sometimes too broad to be analysed and thought in depth.

Finally, the focus is posed on the Intelligence activities for countering new forms of terrorism. The aim is to trace the path the Secret Services have made until now, former underlining the positive aspects and latter showing the difficulties they are finding in adapting their structure to this multiform world.

All these elements are in close dialogue between them. They are different sides of the same coin. It is still quite difficult to regain an equilibrium in this new reality. The International *panorama* is a complex jisgaw puzzle that gives rise to multiple question marks but not to a single exclamation point.