Cyber intelligence, la sfida dei data scientist

di Mario Caligiuri

Abstract

Algoritmi e scenari: il mondo è basato sempre di più sulle previsioni. Per persone, aziende e istituzioni, la rapidità dei mutamenti sociali richiede competenze per anticipare gli eventi, perché chi conosce prima ha un vantaggio competitivo rispetto agli altri. I Big Data costituiscono senza dubbio uno strumento di grande utilità per gli scopi dell'intelligence, e della cyberintelligence in particolare. Per sfruttare le potenzialità dei Big Data è fondamentale che l'intelligence provveda a istituire e formare un team di *data scientist*.

Questo riporta alla ribalta la necessità dell'integrazione dei saperi, richiedendo la fusione di competenze umanistiche e scientifiche. La cyber intelligence è un terreno di analisi, di impegno primario e urgente interesse. Un elemento fondamentale per la cultura della sicurezza.

Profilo dell'autore

Mario Caligiuri è professore straordinario all'Università della Calabria, dove è Direttore del Master in Intelligence e Coordinatore del Centro Studi sull'Intelligence. Insegna nelle alte Scuole delle forze di polizia e del Comparto Intelligence. È stato tra i primi ad introdurre lo studio scientifico dell'intelligence in Italia, promuovendo corsi, master, centri di ricerca, convegni e collane editoriali. Autore di *Cyber Intelligence, tra libertà e sicurezza* (Donzelli), ha curato, tra gli altri, per Rubbettino editore, i testi *Intelligence e scienze umane. Una disciplina accademica per il XXI secolo*; *Intelligence e 'ndrangheta*; *Intelligence. Spie e segreti in un mondo aperto* di Robert D. Steele e *Abecedario*, di Francesco Cossiga.

Keyword

big data, data science

Informazioni e scenari, un continente senza confini

Algoritmi e scenari: il mondo è basato sempre di più sulle previsioni. Per persone, aziende e istituzioni, la rapidità dei mutamenti sociali richiede competenze per anticipare gli eventi, perché chi conosce prima ha un vantaggio competitivo rispetto agli altri. Nei prossimi anni, grazie alla rivoluzione tecnologica, saranno a disposizione sempre maggiori informazioni per assumere decisioni ma questa inedita opportunità, anche se aumenterà la capacità di interpretare i dati, è anche destinata a scontrarsi con i limiti individuali[1] e le imperfezioni strutturali delle

organizzazioni. In questo scenario fluido, di cyber intelligence sentiremo sempre più parlare, perché i conflitti economici, politici e sociali si combatteranno sempre di più attraverso la Rete[2], in un contesto in cui la conoscenza è completamente trasformata.

L'intelligence, inserita nella mediasfera[3], dovrà sviluppare la sua natura di strumento strategico, per decodificare e anticipare gli accadimenti. Tuttavia non è affatto scontato dare una definizione di cyber intelligence: in questa denominazione, infatti, convivono due elementi che operano con logiche differenti. Anzitutto l'intelligenza umana, necessaria alle decisioni, e le tecnologie, che popolano lo spazio digitale. Inoltre oggi non si può prescindere dall'analizzare i grandi agglomerati di informazioni noti come Big Data, che per la loro interpretazione necessiteranno sempre di più della primigenia forma dell'intelligence: quella umana.

L'esistenza di un nuovo continente senza spazio e confini sta radicalmente modificando la vita delle persone e delle istituzioni. Nei prossimi anni sul nostro pianeta le identità virtuali saranno maggiori di quelle fisiche, mentre i dispositivi connessi ad internet nel 2020 potrebbero essere cinquanta miliardi, quattro volte la popolazione mondiale[4]. Tutto ciò imporrà agli Stati di elaborare due distinte politiche: una per le attività nel mondo fisico e un'altra con riferimento a quello virtuale[5], con confini a volte indistinguibili[6]. Secondo Eric Schmidt e Jared Cohen, «la grande maggioranza di noi si troverà sempre più spesso in condizione di vivere, lavorare ed essere governata in due mondi contemporaneamente»[7].

Il cyberspazio moltiplica i fattori di rischio, poiché si sovrappone allo spazio naturale e sociale. I cambiamenti radicali generati dalle nuove tecnologie assumono per l'intelligence una funzione decisiva, tanto che, nell'ambito dello stesso settore, si potrebbe cominciare a ipotizzare una specifica autonomia della cyber intelligence, che è stata così descritta: «Complesso di attività programmate e applicate per identificare, seguire, misurare e monitorare informazioni sulle minacce digitali, nonché dati sulle intenzioni e attività di entità avversarie. Queste attività si svolgono con strumenti cibernetici nel cyberspazio, cioè attraverso la Rete, e hanno una particolarità, a differenza delle altre forme di intelligence: condividono con lo spazio fisico l'uso della human intelligence perché non si può fare totale affidamento alle attrezzature elettroniche»[8].

La cyber intelligence si colloca quindi nell'ambito della cyberwarfare[9], cioè in un ambiente molto più ampio legato ai conflitti nello spazio digitale. In una agorà planetaria dove ci sono ancora poche regole e incertezza nelle collaborazioni[10], la Commissione Europea nel 2013 si è occupata per la prima volta di sicurezza informatica, definendo la *Cyber Security Strategy*[11], in cui auspica un pieno coinvolgimento di cittadini, istituzioni e imprese e promuove la collaborazione internazionale. L'obiettivo deve essere quello di sviluppare una cyber intelligence in cui gli agenti abbiano spiccate «capacità informatiche offensive», perché il cyberspazio sta diventando sempre di più un «settore militare operativo»[12]. In tale situazione, il cosiddetto *web oscuro* rappresenta un terreno di impegno prioritario per la cyber intelligence, poiché consente il reperimento di informazioni a volte indispensabili.

Cyber intelligence e la rivoluzione dei Big Data

Le nuove tecnologie possono determinare una migliore qualità della vita a livello planetario per fasce sempre più ampie di popolazione e, possono concorrere a ridurre la discrezionalità e l'opacità del potere attraverso la trasparenza digitale. In tale scenario, in cui i Big Data stanno assumendo un

ruolo rivoluzionario[13], convivono tendenze opposte. Non a caso, stanno aumentano le incertezze, la solitudine e il disagio delle persone, mentre le istituzioni sono in evidente affanno nel comprendere e adeguarsi ai cambiamenti.

Nel contesto emergente della cyber intelligence è fondamentale considerare la rilevanza della quantità crescente dell'informazione. Le attività che produciamo nel cyberspazio vengono in parte memorizzate e archiviate sotto forma di Big Data[14]. Con questa definizione indichiamo l'enorme e complesso flusso di informazioni in cui «il telefono, la radio e specialmente il computer consentono di tracciare chiunque e ovunque»[15]. Ogni giorno produciamo una grande quantità di dati: clicchiamo su internet e pubblichiamo pensieri sui social network, chiamiamo dal cellulare amici e parenti, comunichiamo tramite email, effettuiamo acquisti con carte di credito, pubblichiamo le nostre diete e condividiamo informazioni intime. Tutte queste attività si svolgono nel cyberspazio ed hanno un effetto collaterale: la produzione di tracce digitali che documentano la nostra vita quotidiana[16].

I Big Data danno oggi forma e sostanza alle attività che svolgiamo nel cyberspazio, divenendo una potentissima lente di osservazione. Siamo alla presenza di un potente *microscopio sociale* che permette di osservare molti aspetti del comportamento umano, sia individuale che collettivo. Esso è tuttavia soltanto uno strumento che monitora le attività nel cyberspazio, poiché i Big Data sono del tutto inutili senza le competenze necessarie per elaborarli, analizzarli e ricavarne conoscenza. Infatti, il termine Big Data, nel suo significato più profondo, si riferisce agli algoritmi matematici per individuare le informazioni e alla creazione di modelli per la previsione delle attività umane[17]. E' importante rilevare che i Big Data non costituiscono un valore in sé, ma lo acquistano grazie alla competenza degli esperti di ricavare informazione utile dall'enorme mole di dati. Il termine Big Data assume quindi un duplice significato, che si riferisce sia alla valanga di dati personali sia all'insieme delle metodologie per trattarli. La consapevolezza di questa rivoluzione[18] comporta una serie di implicazioni psicologiche e sociali, culturali e istituzionali, personali ed economiche[19].

I dati vengono a occupare il centro del palcoscenico. Oggi tutti quei bit[20] digitali che abbiamo raccolto si possono sfruttare con modalità innovative per realizzare nuovi scopi e liberare nuove forme di valore. Ma ciò richiede un nuovo approccio mentale e metterà in discussione le nostre istituzioni e persino il nostro senso di identità»[21]. Questa nuova era sarà caratterizzata da una grande contraddizione, poiché le persone avranno a disposizione sempre più informazioni ma avranno maggiore difficoltà per ricordarle e custodirle.

Grazie ai Big Data che si acquisiscono anche dall'*Internet delle cose*[22] o *Internet del tutto*, l'intelligence, che prima si misurava con il problema spinoso della scarsità, adesso deve affrontare la sovrabbondanza delle informazioni, che solo in minima parte sono disponibili tramite i comuni motori di ricerca o in forma di Big Data. La carenza delle informazioni si è trasformata in eccesso, modificando radicalmente il processo tradizionale di intelligence. Tutto comincia con l'individuazione delle reali esigenze informative dei decisori, che formulano precise richieste[23]. Questa fase delicata è affidata alle figure degli analisti, che utilizzano specifiche metodologie e tecniche per circoscrivere l'esatto fabbisogno informativo[24].

La domanda fondamentale che deve porsi l'analista di intelligence è: qual è l'informazione realmente utile a un preciso decisore politico rispetto a un determinato problema di sicurezza? Si noti che è un aspetto decisivo non solo per l'intelligence ma pervade tutti i contesti della ricerca

sociale[25]. Un aspetto determinante dell'analisi, sin dalle sue prime fasi, è rappresentato dall'individuazione di fonti realmente attendibili, attraverso l'utilizzo di metodi appropriati per valutarne l'affidabilità. A tale ambito, appartiene certamente la *Canadian Check List*[26]. Durante il suo lavoro di indagine, l'analista deve commisurare il livello di precisione della sua attività all'effettivo grado di conoscenza richiesto dal decisore, tenendo conto delle sue competenze sull'argomento. Diventa determinante comprendere i problemi nel dettaglio, analizzandoli con metodi adeguati, per evitare di ricercare informazioni inutili o fuorvianti e avendo presente che internet ha rivoluzionato il *processo tradizionale di analisi* dell'intelligence, poiché ha inciso il modo evidente nella raccolta e nella selezione delle informazioni.

L'individuazione delle informazioni non può peraltro limitarsi al cyberspazio visibile ma deve estendersi al *lato oscuro della Rete*[27] dove, come esposto precedentemente, viaggia una parte preponderante delle informazioni su internet, di grande rilevanza per le attività di intelligence[28]. Analizzare il web, sia quello in superficie che quello oscuro, diventa uno dei pilastri su cui basare le attività di Open Source Intelligence in quanto è possibile ottenere informazioni molto rilevanti non solo con riferimento ai settori della criminalità e del terrorismo, così come a quelli strategici, finanziari e commerciali. Una parte consistente dell'Open Source Intelligence è costituito dai Big Data, dai quali, come evidenziato, è possibile rilevare informazioni predittive assai interessanti per l'intelligence[29].

Attraverso l'esame dei Big Data, l'osservazione delle relazioni sviluppate sui social network o durante le telefonate al cellulare consente la ricostruzione dettagliata della rete delle relazioni personali e l'intensità dei legami. Da qui, l'utilizzo di tecniche proprie della *Network Science*[30] consente facilmente la rilevazione delle principali comunità sociali e persino dei futuri rapporti affettivi delle persone. Tecniche come queste sono state utilizzate per individuare la struttura e l'evoluzione di cellule terroristiche e cosche mafiose, mostrando come sia possibile «identificare, con alta accuratezza, i ruoli degli individui nelle attività criminali dai dati delle loro comunicazioni, semplicemente osservando la struttura delle loro reti sociali»[31]. Il punto vero è che poi occorre utilizzare queste informazioni in modo preventivo e immediato. L'intelligence è indispensabile per comprendere la realtà. E la cyber intelligence lo è ancora di più per orientarsi nella realtà e nel suo doppio: le galassie in espansione del web.

Verso un team di professionisti multidisciplinari

In punto di analisi, i Big Data costituiscono senza dubbio uno strumento di grande utilità per gli scopi dell'intelligence, e della cyberintelligence in particolare, pur tenendo conto che esistono dei limiti nelle previsioni di eventi estremamente complessi, come nel caso del terrorismo fondamentalista[32]. Tuttavia non basta conoscere il fenomeno o averne percezione: occorre cavalcare la tigre. Per sfruttare le potenzialità dei Big Data è fondamentale che l'intelligence provveda a istituire e formare un team di *data scientist*, «una figura che deve avere più competenze […] saper gestire, acquisire, organizzare ed elaborare dati […] sapere come e quali dati estrarre, […] sapere comunicare a tutti, con diverse forme di rappresentazione, cosa suggeriscono i dati»[33].

C'è bisogno di *data scientist*, in lingua amica e al plurale *scienziati dei dati*, che sommano una serie di competenze[34] ma che nel caso specifico dell'intelligence dovrebbe avere uno spiccato orientamento verso l'analisi. Ne consegue che una priorità per l'intelligence nazionale potrebbe essere quella avere a disposizione dei *data scientist*[35], poiché «l'unica certezza è che la quantità di

dati a disposizione continuerà a crescere, di pari passo con la capacità di processarli […]. Possiamo raccogliere e analizzare più informazioni che mai prima d'ora. La scarsità di dati non è più la caratteristica che definisce i nostri tentativi di interpretare il mondo»[36].

Si tratta quindi di preparare operatori con una elevata capacità di contestualizzare le informazioni: nella fase della identificazione di quelle realmente significative, in quella dell'analisi e in quella della distribuzione, in quanto è essenziale *come*, *quando* e *a chi* vengono diffuse le informazioni. In ogni caso, l'esame dei Big Data «richiede una profonda riforma strutturale e mentale (che per alcuni critici potrebbe invece configurarsi come 'declino mentale')[37], oltre a competenze individuali nella selezione e nell'utilizzo delle tecnologie che sono indispensabili per estrarre le previsioni dai Big Data […]»[38].

Vista questa straordinaria importanza, è probabile che nel prossimo futuro il *data scientist*, questa figura professionale multidisciplinare a metà tra l'informatico, lo statistico e l'umanista, potrebbe essere la professione più richiesta al mondo. Non è difficile prevederlo, considerata la crescente necessità da parte di istituzioni e aziende di professionisti che siano in grado di individuare e valorizzare le informazioni preziose nascoste nei Big Data, attraverso algoritmi ed analisi statistiche avanzate[39].

Il nuovo petrolio dell'economia digitale

Va poi evidenziato un ulteriore ostacolo, costituito dall'accesso ai Big Data. Il «nuovo petrolio dell'economia digitale»[40] è dominato quasi esclusivamente da un piccolo gruppo di aziende del cyberspazio come Google, Facebook, Twitter o Amazon e solo una piccola parte di questo patrimonio informativo è visibile e scaricabile dalla Rete[41]. La maggior parte dei dati è nella disponibilità di queste aziende ed è pressoché inaccessibile, salvo rari casi di accordi con università o centri di ricerca per svolgere ricerche sperimentali. I colossi del web non hanno nessun interesse a rendere liberamente disponibili questi dati, da cui ricavano ingenti profitti, vendendo i profili individuali alle società interessate. Per l'accesso ai Big Data, l'intelligence avrà bisogno di stipulare precise intese con questi latifondisti dei dati ed essere disposta a compiere investimenti economici significativi per acquisire questi giacimenti informativi.

Il fattore umano, vero segreto dell'intelligence

Più aumenta l'impatto delle nuove tecnologie e la quantità delle informazioni e più diventa necessario il *fattore umano*[42] dell'intelligence per contestualizzarle[43]. In questa prospettiva, il metodo scientifico è uno strumento indispensabile per avvicinarsi alla comprensione dei fatti. Sul tema esiste una vasta letteratura, in cui si pone il problema di quale metodo scientifico si debba applicare all'intelligence[44], poiché ne esistono diversi tipi, alcuni alternativi tra di loro[45]. Esaminando diverse fonti di informazioni, l'agente di intelligence dovrebbe essere in grado di impiegare «un metodo per trasformare le informazioni in conoscenza»[46], utilizzando il metodo scientifico del tentativo e dell'errore, procedendo per congetture e confutazioni, ipotesi e critiche, pronto a cambiare strategia e opinione di fronte agli imprecisioni, alimentando, tramite l'esperienza e l'istruzione, una mentalità aperta ai cambiamenti. Si impone per l'intelligence «l'esigenza di essere scientifici, non tanto […] nel senso di essere portatori di una scienza esatta, ma come metodo, cioè continuare coerentemente a porre in dubbio ogni cosa, continuare a verificare, essere soprattutto pronti a cambiare idea»[47].

Dal mondo dell'incertezza del passato, siamo oggi nell'epoca delle probabilità, anche se è «molto difficile prevedere ragionevolmente il futuro: siamo infatti nella condizione paradossale in cui gli eventi più importanti […] necessariamente ci sfuggono»[48]. L'intelligence, e la cyber intelligence in particolare, vanno sempre più declinate nell'ambito umano, con regole efficaci ed eticamente corrette, consapevoli delle potenzialità e dei limiti delle tecnologie. Ritorna perciò alla ribalta l'elemento più antico dell'intelligence, quello *umano*, orientato contemporaneamente nell'analisi e nell'operatività, come le recenti vicende di Parigi[49] e di Bruxelles[50] confermano. Possiamo, in teoria, disporre delle più raffinate tecniche di raccolta delle informazioni ma se non vengono analizzate e interpretate tempestivamente per agire sul campo questa complessa attività non fornirà alcun vantaggio. L'analisi dei Big Data ancora oggi non è un processo totalmente automatico e non può prescindere dall'indispensabile supporto umano.

Nello stesso tempo c'è bisogno di elevate competenza informatiche per l'infiltrazione nelle organizzazioni che popolano il web oscuro in modo da tentare di prevenire gli attacchi, impegno necessario per stanare la *galassia del terrore informatico*. Le cyberguerre non si combatteranno solo tra Stati ma saranno sopratutto asimmetriche, con in campo sia Nazioni che organizzazioni criminali e terroristiche, lasciando spazio a conflitti ibridi e ad operazioni di spionaggio sotto mentite spoglie per fare ricadere sugli altri le proprie intenzioni (*false flag*[51]). Quello che conta per l'agente di intelligence è individuare *cosa* ricercare, *come* analizzare e *quando* utilizzare le informazioni richieste. Informazioni che avranno sempre più forma di dati digitali e Big Data, che l'agente dovrà essere in grado di reperire appropriatamente.

In questo percorso di analisi e prevenzione del rischio, non bisogna schierarsi né con gli angeli né con i demoni del web ma utilizzare questi strumenti ponendo al centro i diritti e i valori della persona e finalizzandoli a obiettivi di interesse generale. Bisogna far comprendere alla pubblica opinione, ma soprattutto alla classe dirigente, che lungi dal costituire un insieme di «arti infernali»[52], l'intelligence rappresenta invece uno strumento fondamentale di prevenzione dei conflitti. Con indubbi benefici umani ed economici. Infine c'è il tema della formazione, che deve essere fortemente innovativa ma sempre partendo dall'istruzione tradizionale di base, ampliata con nuovi ed efficaci metodi, evitando illusioni pedagogiche[53]. La complessità dei temi trattati, dai Big Data dalla cyber intelligence, evidenziano ancora una volta l'importanza del fattore umano.

Nel film di James Bond *Skyfall* c'è un dialogo illuminante che si svolge in un museo davanti a un quadro tra Q, l'inventore delle innovazioni tecnologiche più avanzate, per la prima volta interpretato da un giovanissimo agente, e il maturo James Bond. Il confronto è anch'esso la 'spia' di un sentire:

Q: *Dà sempre una certa malinconia. Una grandiosa nave da guerra trainata ingloriosamente alla demolizione. L'ineluttabilità del tempo, ti pare? Tu cosa vedi?*

007: *Tanta acqua e una barca. Mi scusi [e si alza per andarsene].*

Q: *007 sono il nuovo addetto all'approvvigionamento.*

007: *Stai scherzando, spero.*

Q: *Perché non ho camici da laboratorio?*

007: No, perché hai ancora i brufoli.

Q: La mia epidermide non è affatto rilevante.

007: Ma la tua competenza sì.

Q: L'età non è una garanzia di efficienza.

007: E la giovinezza non è una garanzia di innovazione.

Q: Oso dire che faccio molti più danni io con il mio portatile[54] in pigiama seduto davanti alla prima tazza di Earl Grey di quanti ne fai tu in un anno sul campo.

007: Oh. E a che vi servo, allora?

Q: Ogni tanto un grilletto va premuto.

007: O non premuto. È difficile scegliere se sei in pigiama.[55]

Darknet e nuove frontiere della minaccia, il ruolo del DIS

La natura destrutturata dell'ambiente digitale sollecita l'intelligence confrontarsi con un cambiamento strutturale, poiché è nella stessa rete che bisogna interagire per prevenire la minaccia. La Relazione annuale sulla politica dell'informazione per la sicurezza 2015, pubblicata su www.sicurezzanazionale.gov.it, il sito del Comparto intelligence, spiega che «la rivoluzione cibernetica è suscettibile di incidere profondamente sul modo di fare intelligence. Si configura come 'la' nuova frontiera, che cambia ogni fase e la natura stessa del processo informativo, ed impone un radicale cambio di abito mentale nella risposta, che deve essere veloce, organica, e preventiva».

Un altro dato è inconfutabile: il cyberspazio non ammette approssimazioni. Con interessanti prospettive[56], il nostro Paese, rendendo operativi gli accordi europei, ha adottato alcuni atti[57], per delineare strutture e competenze di una politica nazionale nel settore[58]. Il Dipartimento delle Informazioni per la Sicurezza (DIS) ha fornito uno specifico contributo[59], evidenziando le tendenze della minaccia informatica, la vulnerabilità delle infrastrutture tecnologiche, gli strumenti e le procedure per rafforzare la capacità di difesa, individuando ruoli e compiti del settore pubblico[60]. Con i vari provvedimenti governativi, all'intelligence nazionale, e soprattutto al Dipartimento delle Informazioni per la Sicurezza sono stati attribuiti ruoli precisi[61].

Da qualche tempo, come si ricorderà, è stato costituito presso l'Agenzia Informazioni e sicurezza interna un apposito reparto che si occupa di tale settore col compito di collegarsi con i servizi di intelligence stranieri e con istituzioni pubbliche e private nazionali. Tutto ciò richiede l'efficienza del nostro sistema di intelligence, poiché sarebbe funzionale che fosse un unico organismo a collaborare sia all'estero con le altre agenzie di intelligence che all'interno con le strutture pubbliche e private nazionali. I compiti assegnati all'intelligence sono impegnativi e richiedono procedure, strumenti e modalità di azione profondamente diversi rispetto a quelli finora utilizzati.

Questo vale dall'analisi dei pericoli al trattamento delle informazioni[62], dal contrasto al cybercrime allo sviluppo di capacità operative[63]. Si tenga sempre conto, del resto, dell'estrema difficoltà di individuare l'origine di attacchi informatici che possono venire commissionati da Stati,

organizzazioni criminali, terroristiche o altri soggetti, a circa un centinaio di organizzazioni che rappresentano un mercato *underground*: «la Tortuga di questi pirati invisibili si nasconde nel darkne*t*, la zona oscura di internet, inaccessibile agli utenti comuni»[64]. Per contrastare in modo preventivo queste minacce e individuare origine, scopo e conseguenze dei crimini informatici, l'azione più efficace si conferma ancora l'intelligence umana.

Di fronte all'ampiezza del rischio, c'è bisogno di strumenti legislativi e iniziative significative, vista l'ampiezza e l'indistinta pluralità della minaccia. Il rischio maggiore, però, proviene spesso da singoli e insospettabili individui che possono adoperarsi per acquisire dati sensibili dal punto di vista politico ed economico o danneggiare le infrastrutture digitali nazionali, dalle quali dipende l'organizzazione e lo sviluppo della comunità. In tale scenario, è rilevante la funzione preventiva dell'intelligence, poiché serve a contrastare un nuovo spazio di azione della criminalità e del terrorismo, oltre che dello spionaggio economico.

Citizen intelligence

La vastità e la frequenza dei dati, il numero dei loro produttori e utilizzatori espone a evidenti rischi per cui le città possono essere oggetto di specifici attacchi informatici. Perciò va utilizzato in contemporanea l'anticorpo della cyber intelligence, non solo attraverso precise previsioni e azioni ma soprattutto progettando le tecnologie delle *smart cities* fin dall'inizio con il coinvolgimento diretto dei cittadini[65]. Tale procedimento può risultare di grandissima utilità poiché consente di integrare le previsioni di intelligence per rendere le procedure meno violabili.

La partecipazione attiva della popolazione per prevenire le minacce informatiche rappresenta un'estensione del concetto della *citizen intelligence*[66], in base al quale ogni singolo cittadino è contemporaneamente fruitore e produttore di intelligence. In questa dimensione, il cittadino è inteso come baluardo per anticipare le minacce informatiche ovvero può essere considerato a tutti gli effetti un *volontario dell'intelligence*, sia per anticipare che per riparare i danni provocati.

Una prospettiva aperta

La formazione delle figure dei *data scientist* diventa fondamentale, essendo indispensabile fondere le competenze scientifiche con quelle umanistiche, perché il sapere è globale e la sua suddivisione specialistica ha comportato nello stesso tempo progressi e perdite. Vanno sviluppati approfondimenti nei settori delle tecnologie, delle scienze cognitive e perfino dei saperi considerati non scientifici[67]. L'efficace e immediato utilizzo dell'informazione che potrà conferire alle élite pubbliche gli strumenti adatti per contrastare seriamente quelle criminali e terroristiche. Va promossa nel nostro Paese la cultura dell'intelligence, dove peraltro esistono una serie di pregiudizi e luoghi comuni[68] che rappresentano le tesi «sulle quali si discute ma sulle quali non si discute»[69].

Nella *guerra economica* che caratterizza la globalizzazione, dove le nazioni non sono più alleate o avversarie, ma semplicemente, caso per caso, concorrenti, si richiederanno quantità sempre maggiori di cyber intelligence. Come sempre, l'impegno non può che essere culturale nel senso della corretta identificazione dei fenomeni per poter approntare le azioni più opportune. In uno scenario che è destinato ad essere sempre più fluido, la cyber intelligence può rappresentare un luogo di sperimentazione tra le libertà individuali e la sicurezza generale, alla ricerca di un difficile ma indispensabile punto di equilibrio.

Proprio questo settore, richiedendo la presenza di figure specializzate come i *data scientist*, riporta alla ribalta la necessità dell'integrazione dei saperi, richiedendo la fusione di competenze umanistiche e scientifiche e ritornando al concetto unitario di cultura, in opposizione a quanto sta avvenendo nella frantumazione della conoscenza, motivo non ultimo del disagio e della confusione dell'uomo contemporaneo. La cyber intelligence è un terreno di analisi, di impegno primario e urgente interesse. Un elemento fondamentale per la cultura della sicurezza.

Note

(ultimo accesso ai link indicati: 22 giugno 2016)

[1] A metà degli anni Cinquanta del Novecento, l'economista Herbert A. Simon ha elaborato la teoria delle 'decisioni a razionalità limitata', secondo la quale le persone non riescono a scegliere in modo logico poiché condizionate da tre circostanze: l'impossibilità di possedere tutte le informazioni, i limiti cognitivi individuali, i tempi limitati per assumere le decisioni. Tutto questo fa si che più che le scelte 'ottimali' vengano adottate quelle 'soddisfacenti'. Tra gli altri, dello stesso autori vedi H.A. SIMON, *La ragione nelle vicende umane*, Il Mulino, Bologna 1984.

[2] E. SCHMIDT, J. COHEN, *La nuova era digitale. La sfida del futuro per cittadini, imprese e nazioni*, Rizzoli Etas, Milano 2013, p. 123.

[3] Termine coniato da Régis Debray per descrivere la caratteristiche dell'epoca contemporanea in cui la presenza dei media condiziona comportamenti e decisioni delle persone, così come quelle delle organizzazioni pubbliche e private.

[4] H. KISSINGER, *Ordine Mondiale*, Mondadori, Milano 2015, p. 340.

[5] Schmidt, Cohen, *La nuova era digitale,* cit., pp. 25-93.

[6] Interessante il caso dell'Estonia che consente la possibilità di residenze digitali.

[7] Schmidt, Cohen, *La nuova era digitale. La sfida del futuro per cittadini, imprese e nazioni*, cit., p. XV.

[8] *Information Warfare 2011. La sfida della Cyberintelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, a cura di U. Gori, L.S. Germani, Franco Angeli, Milano 2012, pp. 16-17.

[9] La *Cyberwar* è l'attività e modalità di combattimento attraverso gli strumenti informatici mentre la *Cyber warfare* oltre alla guerra è anche tutto ciò che vi sta intorno: dottrine, teorie, modalità logistica e strumenti diversi. L'*Information Warfare* è suddivisa in: *Command and Control Warfare* (che mira a colpire il centro di controllo e comando dell'avversario), *Intelligence Basic Warfare* (che cerca di inquinare la gestione dell'informazione dell'avversario e proteggere la propria), *Electronic Warfare* (che utilizza strumenti radio, elettronici e crittografici), *Psychological Warfare* (che tende a influenzare le opinioni di persone e comunità), *Hacker Warfare* (che riguarda gli attacchi alle reti telematiche), *Economic Information Warfare* (che attiene alla sicurezza e agli interessi economici nazionali). In tale situazione, la *Cyber warfare* rappresenta il complesso di tutte le operazioni con l'utilizzo delle più importanti e avanzate tecnologie.

[10] Il Presidente americano Barack Obama ha definito il Cyberspace come un 'wild west' e il 13.2.2015 ha emanato un Executive Order per promuovere la collaborazione tra pubblico e privato in questo settore strategico.

[11] http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm.

[12] A. FLORES D'ARCAIS, *USA: la nuova guerra è il cyber-spazio*, http://inchieste.repubblica.it/it/repubblica/rep-it/2015/06/15/news/cosi_mi_arruolo_tra_gli_007-115409472/#Usa.

[13] V.MAYER-SCHÖNBERGER, K. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, Milano 2013.

[14] Il termine Big enfatizza la dimensione (grande) dei dati, ma i Big Data sono caratterizzati dalle quattro V: volume, varietà, velocità e veridicità. Queste servono ad indicare anche la complessità dei Big Data e quindi anche la difficoltà di gestirli e analizzarli.

[15] S. LEVY, *Crypto: How the code rebels beat the government-saving privacy in the digital age*, Penguin USA, 2001.

[16] Una valida fonte per la comprensione delle tracce digitali e le fonti di Big Data è S. BAKER, *The Numerati*, Houghton Mifflin Co., Boston 2008. L'edizione italiana è S. BAKER, *Il potere segreto dei matematici. Chi sono i signori dei numeri che controllano il nostro comportamento: cosa compriamo, come votiamo, chi amiamo*, Mondadori, Milano 2010.

[17] In questo caso di può parlare di Big Data Analysis o Big Data Analytics per descrivere le operazioni di analisi dei Big Data rivolte all'individuazione di tendenze, modelli, caratteristiche non esplicite attraverso l'approfondimento delle informazioni.

[18] «Il fenomeno dei Big Data segna l'inizio di una trasformazione radicale», Mayer-Schönberger, Cukier, *Big Data,* cit., p. 16.

[19] «I Big Data saranno una fonte di nuovo valore economico e d'innovazione». Mayer-Schönberger, Cukier, *Big Data,* cit. p. 24.

[20] In questo caso il termine Bit è l'unità di misura dell'informazione quindi, in senso lato, la quantità delle informazioni.

[21] Mayer-Schönberger, Cukier, *Big Data,* cit., p. 258.

[22] Con la definizione *Internet delle Cose* (Internet of Things) si intendono «le tecnologie che collegano tramite la Rete gli oggetti fisici direttamente tra loro, venendo monitorati, controllati e guidati». Come esempi, Antonio Teti cita «il frigorifero che avvisa l'utente quando si avvicina la data di scadenza di un prodotto deteriorabile oppure la sveglia che comunica alla macchinetta del caffè di attivarsi»[22], ma le applicazioni possono essere infinte. A. TETI, *Open Source Intelligence & Cyberspace. La nuova frontiera della conoscenza*, Rubbettino, Soveria Mannelli 2015, pp. 53-54.

[23] Il ciclo dell'intelligence secondo Mark M. Lowenthal deve essere necessariamente anticipato dall'individuazione del fabbisogno informativo del decisore. Vedi M.M. LOWENTHAL, *Intelligence, From Secrets to Policy*, CQ Press, Washington 2000.

[24] Come la *Five WS-and-H* e il *Question Method*. Vedi A. TETI, *Open Source Intelligence & Cyberspace.* La *nuova frontiera della conoscenza*, cit., pp. 68-70.

[25] A. GOLDMAN, *Knowledge in a Social World,* Oxford University Press, Oxford 1999, pp. 318-348.

[26] Teti, *Open Source Intelligence & Cyberspace*, cit., pp. 117-120. Messo a punto dal governo canadese, si tratta di una ventina di voci da verificare, per compilare le quali occorre tempo, prima di tutto, e poi anche competenze specifiche che consentano una corretta valutazione delle fonti. Vedi anche le precedenti pp. 109-114.

[27] N. CARR, *Il lato oscuro della Rete. Libertà, sicurezza, privacy,* Etas, Milano 2008. Sul cosiddetto 'lato oscuro della Rete' ci sono diverse pubblicazioni, tra le quali E. MOROZOV, *L'ingenuità della Rete. Il lato oscuro della libertà di internet,* Codice, Torino 2011*;* A. GRANELLI, *Il lato oscuro del digitale. Breviario per sopravvivere nell'era della Rete,* Franco Angeli, Milano 2013*;* R. MEGGIATO, *Il lato oscuro della Rete. Alla scoperta del Deep Web e del Bitcoin,* Apogeo, Milano 2014.

[28] «All'interno del Deep Web troviamo prevalentemente *siti occultati* che non sono visualizzabili con delle semplici ricerche con Google, ma che possono essere visti solo utilizzando delle tecniche di navigazione particolari in grado di garantire dei livelli di riservatezza elevati». Teti, *Open Source Intelligence & Cyberspace*, cit., p. 234. Successivamente nel libro si legge che «Sono innumerevoli i siti web e i servizi offerti forniti dal circuito del portale Tor. Uno di questi è Grams (raggiungibile con il browser Tor al seguente indirizzo http://grams7enufi7jmdl.onion), altrettanto famoso per le sue attività illecite ma altresì in grado, primo fra tutti, di indicizzare i prodotti illegali messi in vendita in questa Rete riservata». Teti,

Open Source Intelligence & Cyberspace, p. 245-246. Tra i siti più interessanti del Deep Web, vanno citati Hidden Wiki e Silk Road, v. Teti, *Open Source Intelligence & Cyberspace*, p. 239.

[29] F. VITALI, *L'oro nero dei dati*, in «Limes», *A che servono i servizi*, Luglio 2014, pp. 29-36.

[30] La network science (scienza delle reti) è una disciplina che si occupa dello studio delle reti complesse come le reti di telecomunicazioni, le reti biologiche, Internet, e le reti sociali. Per un'introduzione alla Network Science si veda il libro di A.-L. BARABASI, *Link. La scienza delle reti*, Einaudi, Torino 2004, edizione originale *Linked: the New Science of Networks*, Perseus Publishing, 2002 -

[31] N. UNGERLEIDER, *Mafia wars: how Italy's military police use metadata to track organized crime*, Fast Company, http://www.fastcompany.com/3029152/mafia-wars-how-italys-secret-police-use-metadata-to-track-organized-crime.

[32] La difficoltà di effettuare previsioni tramite dati derivati da internet emerge in maniera estremamente chiara e drammatica nella conferenza *The Islamic State's Ideology and Propaganda* promossa dalla Brookings Institution l'11 marzo 2015, rivenibile www.youtube.com/watch?v=-Coyrop8G2s. In particolare, nell'intervento di J.M. Berger e Jonathon Morgan sul loro saggio *The ISIS Twitter Census. Defining and describing the population of ISIS supporters on Twitter,* http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

[33] *Professione scienziato del dato*, Nova24 Tech, «Il Sole24Ore», 26 ottobre 2014, http://www.ilsole24ore.com/art/tecnologie/2014-10-26/professione-scienziato-dato-081257.shtml?uuid=ABHDEu6B.

[34] Una prima parziale descrizione, orientata principalmente sul settore privato e che si limita soprattutto agli aspetti tecnologici ed economici, ha cercato di darla Thomas H. Davenport. «La figura classica del data scientist presenta cinque volti: hacker, scienziato, analista quantitativo, consulente di fiducia, esperto di business». Th.H. DAVENPORT, *Big Data @l lavoro. Sfatare i miti, scoprire le opportunità*, Franco Angeli, Milano 2015, p. 86.

[35] A. TETI, *I Data Scientist. Una risorsa per l'intelligence*, in «GNOSIS, Rivista Italiana di Intelligence», n. 3-2012, pp. 45-63, http://gnosis.aisi.gov.it/Gnosis/Rivista32.nsf/ServNavig/32-07.pdf/$File/32-07.pdf?OpenElement.

[36] Mayer-Schönberger, Cukier, *Big Data*, cit., p. 258.

[37] M. CALIGIURI, *Introduzione*, in Teti, *Open Source Intelligence & Cyberspace*, cit., p. 15.

[38] M. CALIGIURI, *Intelligence: svelare le menzogne nella penombra dei Big Data*, 2015, http://www.aspeninstitute.it/aspenia-online/article/intelligence-svelare-le-menzogne-nella-penombra-dei-big-data.

[39] TH. H. DAVENPORT, D.J. PATIL, *Data Scientist: The Sexiest Job of the 21st Century*, ottobre 2012, https://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century/

[40] «I dati per il XXI secolo sono come il petrolio per il XVIII secolo: un bene immensamente prezioso ma ancora non sfruttato. Proprio come il petrolio, per coloro che riescono a carpire il valore fondamentale dei dati, ad estrarlo e a sfruttarlo ci saranno enormi benefici economici», in *Data is the new oil of digital economy*, in «Wired», luglio 2014, http://www.wired.com/insights/2014/07/data-new-oil-digital-economy/.

[41] Alcune aziende, come Twitter e Facebook, forniscono un accesso ristretto ad una piccola parte dei dati attraverso le cosiddette Application Programming Interface (API), un insieme di protocolli e strumenti per la costruzione di applicazioni software per lo scaricamento dei dati memorizzati sul Web.

[42] G. GREENE, *Il fattore umano*, Mondadori, Milano 1978. *Il fattore umano* è il titolo di un libro di Graham Greene che racconta la fondamentale importanza del fattore umano nel mondo dello spionaggio. Ambientato durante la guerra fredda, l'opera dello scrittore inglese mette in evidenza come il comportamento umano rappresenti un elemento imprevisto e imprevedibile che neppure l'analisi più accurata potrebbe riuscire a identificare. Dal libro nel 1979 è stato tratto l'omonimo film diretto da Otto Preminger.

[43] «[…] c'è una generale concordanza sul fatto che l'elemento umano sia operativamente e strategicamente centrale e dominante anche nella cyber guerra e nel più ampio mondo della cyber sicurezza», G. PILI, *Filosofia pura della guerra*, Aracne, 2015, p. 475. In quest'opera del giovane ricercatore dell'Università Vita-Salute San Raffaele di Milano convergono una pluralità di apporti disciplinari dai quali emerge che l'elemento umano rimane fondamentale anche nelle guerre contemporanee caratterizzate dall'altissimo impatto tecnologico.

[44] I. BEN ISRAEL, *Philosophy and methodology of intelligence: The logic of estimate process,* in «Intelligence and National Security», n. 4/1989, pp. 660-718. Lo studioso israeliano propone un metodo per l'intelligence che si fonda sulla costruzione di teorie alternative che poi vanno progressivamente scartate, ampliando e contaminando i concetti di Karl Popper, per produrre un metodo che sia scientifico e applicabile alle esigenze specifiche dell'intelligence.

[45] Tra questi, il metodo verificazionista, quello falsificazionista di Karl Popper, oltre alla logica della ricerca scientifica di Thomas Kuhn e alle argomentazioni 'contro il metodo' di Paul Feyerabend.

[46] D. ANTISERI, A. SOI, *La scienza dell'intelligence nell'era dell'incertezza*, Rubbettino-Formiche, Supplemento a «Formiche», n. 99, gennaio 2015.

[47] G. MASSOLO in Antiseri, Soi, *La scienza dell'intelligence nell'era dell'incertezza*, cit. p. 29.

[48] F. ANTINUCCI, *L'algoritmo al potere. Vita quotidiana ai tempi di Google*, Laterza, Roma-Bari 2009, p. 4.

[49] Ci riferiamo ai sanguinosi episodi accaduti a Parigi ad opera del terrorismo islamico il 7 gennaio 2015 nella redazione del giornale satirico *Charlie Hebdo* e quelli avvenuti il 13 novembre 2015 al teatro Bataclan, allo Stade de France e in altri luoghi della città.

[50] Il 22 marzo 2016 a Bruxelles intorno alle ore 8 si sono verificati due attentati presso l'aeroporto di Zaventem e uno alla stazione della metropolitana di Maalbeek, causando 34 morti e 200 feriti. La stage è stata rivendicata dall'IS.

[51] Per false flag (bandiera falsa) si intendo operazioni compiute da Nazioni e agenzie di intelligence sia in tempi di pace che in periodi di guerra. Va precisato che le operazioni *sotto falsa bandiera* sono utilizzate non solo nello spionaggio governativo e industriale, ma anche nel marketing (con campagne di relazioni pubbliche) e nella politica (con iniziative propagandistiche ed elettorali).

[52] La definizione è di Immanuel Kant in *Per la pace perpetua* con riferimento alle azioni degli Stati durante le guerre che finiscono poi con il compromettere le relazioni tra gli Stati anche in tempo di pace. I. KANT, *Per la pace perpetua*, Feltrinelli, Milano 1991. L'edizione originale in tedesco è del 1795.

[53] P. MASTROCOLA, *Scusate il disturbo. Saggio sulla libertà di non studiare,* Guanda, Parma 2012; F. FUREDI, *Fatica sprecata. Perché la scuola di oggi non funziona*, Vita e Pensiero, Milano 2012.

[54] «Un computer portatile può produrre conseguenze globali. Una singola persona che disponga di una sufficiente potenza di calcolo è in grado di accedere al cyberdominio e di disabilitare, e potenzialmente distruggere, infrastrutture essenziali da una posizione di anonimato pressoché assoluto», v. Kissinger, *Ordine Mondiale*, cit., p. 342.

[55] S. Torani, Quando il cielo crolla. Trauma e immaginario post mortem in Skyfall, , Tesi di laurea in storia del cinema, a.a. 2013/2014, http://www.academia.edu/15443296/Quando_il_cielo_crolla_trauma_e_immaginario_post-mortem_in_Skyfall_

[56] R. BALDONI, R. DE NICOLA, *Il Futuro della Cyber Security in Italia Un libro bianco per raccontare le principali sfide che il nostro Paese dovrà affrontare nei prossimi cinque anni*, Laboratorio Nazionale di Cyber Security-Consorzio Interuniversitario Nazionale per l'Informatica, ottobre 2015. http://www.consorzio-cini.it/index.php/it/component/attachments/download/416.

[57] Si tratta del DPCM del 24 gennaio 2013, http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2013/03/dpcm-24-01-2013.pdf.

[58] Si fa riferimento al *Quadro Strategico Nazionale* che delinea il corrispondente *Piano Nazionale*, https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html.

[59] Nel dicembre del 2013 è stato predisposto il documento *National Strategic Framework For Cyberspace Security*, rinvenibile in www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.

[60] Vengono definite le azioni di pertinenza della Presidenza del Consiglio dei Ministri e dei Ministeri di Esteri, Interni, Difesa, Economia, Sviluppo Economico.

[61] Al Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei Ministri viene assegnato un ruolo centrale poiché, tramite il proprio Direttore, coordina le attività per garantire la sicurezza informatica nazionale; è responsabile delle attività di ricerca e di elaborazione informativa, formulando analisi, valutazioni e previsioni sulla minaccia cibernetica; raccoglie informazioni, le elabora e le diffonde; promuove, tra i decisori pubblici ma anche quelli privati, la consapevolezza e la conoscenza dei rischi della minacce informatiche, evidenziando le possibili attività di contrasto; redige il Documento di Sicurezza Nazionale sulle alle attività per il contrasto alla minaccia cibernetica, allegandolo alla relazione annuale al Parlamento; stipula, insieme alle Agenzie, apposite convenzioni con pubbliche amministrazioni, università, centri di ricerca e soggetti erogatori di servizi di pubblica utilità, anche accedendo ai loro archivi informatici.

[62] Si fa riferimento a *cyberintelligence* e *knowledge management*.

[63] Secondo le direttive della difesa sull'ambiente cibernetico (Centro Operativo Cibernetico Interforce - Coci).

[64] G. MICALESSIN, *Hacker scatenati, Italia primo bersaglio*, in «Il Giornale», 3 febbraio 2013, http://www.ilgiornale.it/news/esteri/hacker-scatenati-italia-primo-bersaglio-881695.html.

[65] Non si possono costruire smart cities senza che gli stessi cittadini abbiano le competenze e collaborino, in quanto non basta la tecnologia poiché il fattore umano rimane fondamentale. D. TALIA, *Una città può essere smart se non è umana?,* in «Il Quotidiano della Calabria», 21 dicembre 2013.

[66] Sul concetto di *citizen intelligence*, vedi R.D. STEELE, *Intelligence. Spie e segreti in un mondo aperto*, Rubbettino, Soveria Mannelli 2003.

[67] Nel testo abbiamo evidenziato esperimenti compiuti dai servizi segreti durante la guerra fredda, come le spie psichiche e la visione remota. E può essere utile indagare temi come la parapsicologia e anche l'antica sapienza dell'alchimia così come punti di vista alternativi. A questo riguardo è interessante, con qualche riserva, M. PIZZUTI, *Scoperte scientifiche non autorizzate*, Il Punto d'Incontro, Vicenza 2011.

[68] Un elenco incompleto ma significativo sui pregiudizi sull'intelligence nella società italiana vedi M. CALIGIURI, *Università e intelligence. Un punto di vista italiano*, in «Per Aspera ad Veritatem», anno IX, n. 25, gennaio-aprile 2003, pp. 85-108, http://gnosis.aisi.gov.it/sito%5CRivista25.nsf/servnavig/5.

[69] P. BORDIEU, L. WACQUANT, *Astuzie della ragione imperialista*, in *Le astuzie del potere. Pierre Bordieu e la politica democratica*, a cura di L. Wacquant, ombre corte, Verona 2005, p. 161.